Payment Card Industry
データセキュリティ基準

要件とテスト手順

v4.0

2022 年 3 月

文書の変更

日付	バージョン	説明
2008 年 10 月	1.2	PCI DSS v1.2 を『PCI DSS 要件とセキュリティ評価手順』として紹介するために、ドキュメント間の重複を削除し、『PCI DSS セキュリティ評価手続き v1.1』からの一般的な変更および固有の変更を行った。詳細については、『PCI データセキュリティ基準: PCI DSS バージョン 1.1 から 1.2 への変更点のまとめ』を参照してください。
2009 年 7 月	1.2.1	PCI DSS v1.1 と v1.2 の間で誤って削除された文章を追加しました。
		テスト手順 6.3.7.a および 6.3.7.b の「then」を「than」に修正しました。
		テスト手順 6.5.b の「対応」と「未対応」のグレイアウトのマーキングを削除しました。
		「代替コントロールワークシート – 完成例」の、ページの一番上の文を「このワークシートを使用して、 代替コントロールにより『対応』と記載された要件について代替コントロールを定義します。」に修正しました。
2010 年 10 月	2.0	v1.2.1 からの変更点を更新および反映。詳細については、『PCI DSS - PCI DSS バージョン 1.2.1 から 2.0 への変更点のまとめ』を参照してください。
2013 年 11 月	3.0	v2.0 からの変更点を更新。詳細については、『PCI DSS - PCI DSS バージョン 2.0 から 3.0 への変更点のまとめ』を参照してください。
2015 年 4 月	3.1	v3.0 からの変更点を更新。詳細については、『PCI DSS – PCI DSS バージョン 3.0 から 3.1 への変更点のまとめ』を参照してください。
2016 年 4 月	3.2	v3.1 からの変更点を更新。詳細については、『PCI DSS – PCI DSS バージョン 3.1 から 3.2 への変更点のまとめ』を参照してください。
2018 年 5 月	3.2.1	v3.2 からの変更点を更新。詳細については、『PCI DSS – PCI DSS バージョン 3.2 から 3.2.1 への変更点のまとめ』を参照してください。

日付	バージョン	説明
2022 年 3 月	4.0	文書のタイトルを「Payment Card Industry Data Security Standard」に変更する。要件とテスト手順" に変更。 PCI DSS v3.2.1 からの更新。変更の詳細については、「PCI DSS - PCI DSS Version 3.2.1 から 4.0 への変更点の概要」を参照してください。

免責事項：本文書の英語版は、PCI SSC ウェブサイト上で利用可能になっており、全ての目的において、これらの文書の正規版と見做される。

本記述と英語版記述との間に曖昧もしくは不一致がある限りにおいては該当部分に相当する英語版が優先される。

目次

1 概論および PCI データセキュリティ基準の概要

Payment Card Industry データセキュリティ基準（PCI DSS）は、ペイメントカードのアカウントデータのセキュリティを推進および強化し、均一なデータセキュリティ評価基準の採用をグローバルに進めるために策定されました。PCI DSS は、アカウントデータを保護するために設計された技術面および運用面の要件のベースラインとして利用できます。PCI DSS は、ペイメントカードのアカウントデータを扱う環境に特化して設計されていますが、ペイメントシステム全体の他の要素を脅威から保護するためにも使用できます。

表 1 に、PCI DSS の主な 12 要件を示します。

表 1。主な PCI DSS 要件

PCI データセキュリティ基準の概要	
安全なネットワークとシステムの構築と維持	**1.** ネットワークのセキュリティコントロールを導入し、維持します。 **2.** すべてのシステムコンポーネントに安全な設定を適用します。
アカウントデータの保護	**3.** 保存されたアカウントデータを保護します。 **4.** オープンな公共ネットワークでカード会員データを伝送する場合、強力な暗号化技術でカード会員データを保護します。
脆弱性管理プログラムの維持	**5.** すべてのシステムとネットワークを悪意のあるソフトウェアから保護します。 **6.** 安全性の高いシステムおよびソフトウェアを開発し、保守します。
強力なアクセス制御手法の導入	**7.** システムコンポーネントおよびカード会員データへのアクセスを、業務上必要な適用範囲に制限します。 **8.** ユーザを識別し、システムコンポーネントへのアクセスを認証します。 **9.** カード会員データへの物理的なアクセスを制限します。

PCI データセキュリティ基準の概要	
ネットワークの定期的な監視およびテスト	**10.** システムコンポーネントおよびカード会員データへのすべてのアクセスを記録し、監視します。 **11.** システムおよびネットワークのセキュリティを定期的にテストします。
情報セキュリティポリシーの維持	**12.** 事業体のポリシーとプログラムにより、情報セキュリティを維持します。

本書『PCI データセキュリティ基準要件およびテスト手順』は、PCI DSS の 12 の主要要件、セキュリティ要件の詳細、対応するテスト手順、および各要件に関連するその他の情報で構成されています。以下のセクションでは、PCI DSS 評価の準備、実施、および結果の報告を行う事業体を支援する詳細なガイドラインとベストプラクティスを提供します。PCI DSS 要件およびテスト手順は、44 ページ以降に記載されています。

PCI DSS はアカウントデータを保護するための最小限の要件で構成され、リスクを軽減する追加の規制や慣行、さらには地元、地域、セクターの法規制によって強化される場合があります。さらに、法律または規制上の要件により、個人情報またはその他のデータ要素（カード会員名など）の特定の保護が必要になる場合があります。

制限事項

本書に含まれる要件のいずれかが国、州、または地域の法律と矛盾する場合、国、州、または地域の法律が適用されます。

PCI DSS のリソース

PCI Security Standards Council（PCI SSC）のウェブ サイト（www.pcisecuritystandards.org ）には、事業体が PCI DSS の評価と検証を行う際に利用できる以下の関連リソースが掲載されています。

- ドキュメントライブラリ（以下を含む）：
  - PCI DSS 変更点のまとめ

  - PCI DSS クイックリファレンスガイド
  - 補足情報とガイドライン PCI DSS の優先的なアプローチ
  - 準拠に関するレポート（ROC）テンプレートおよび報告書作成の手引き
  - 自己問診票（SAQ）および SAQ の手引きとガイドライン
  - 準拠証明書（AOC）
- よくある質問（FAQ）
- 小規模加盟店向けの PCI ウェブサイト
- PCI トレーニングコースおよび情報提供のためのウェビナー
- 認定セキュリティ評価者（QSA）および認定スキャニングベンダ（ASV）のリスト
- PCI が承認したデバイス、アプリケーション、およびソリューションのリスト

PCI SSC の ウェブサイトには、PCI DSS に関する具体的なガイダンスや考慮事項を記載した 60 以上のガイダンス文書と補足資料が公開されています。例としては、以下のようなものがあります。

- PCI DSS の適用範囲とネットワークセグメンテーションのためのガイダンス
- PCI SSC クラウドコンピューティングガイドライン
- 多要素認証ガイダンス
- サードパーティにおけるセキュリティの保証
- 効果的な日次のログレビュ
- ペネトレーションテストのガイダンス
- セキュリティ教育プログラムのベストプラクティス
- PCI DSS 準拠を維持するためのベストプラクティス
- 大規模な事業体における PCI DSS
- SSL／初期の TLS の使用と ASV スキャンへの影響
- POS POI 端末接続における SSL／初期の TLS の利用
- トークン化製品のセキュリティガイドライン

*__注意：__ 補足情報は **PCI DSS** を補完し、**PCI DSS** 要件を満たすための追加の検討事項や推奨事項を特定するものであり、**PCI DSS** またはその要件のいずれかを代替・拡張するものではありません。*

- 電話決済におけるカード情報の保護

上記の情報およびその他の資料については、ドキュメントライブラリ（www.pcisecuritystandards.org ）を参照してください。

また、PCI DSS における用語の定義については、付録 G を参照してください。

2 PCI DSS 適用情報

PCI DSS は、カード会員データ（CHD）や機密認証データ（SAD）を保存、処理、または伝送するすべての事業体と、カード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるすべての事業体を対象としています。これには、加盟店、プロセサー、アクワイアラ、イシュア、その他のサービスプロバイダを含む、カード情報の処理に関与するすべての事業体が含まれます。

事業体が PCI DSS への準拠または準拠の検証を必要とするかどうかは、準拠プログラムを管理する組織（ペイメントブランドやアクワイアラなど）の判断により決定されます。追加の基準については、関連する組織にお問い合わせください。

アカウントデータ、カード会員データ、機密認証データの定義

カード会員データと機密認証データはアカウントデータとされ、以下のように定義されています。

表 2。アカウントデータ

アカウントデータ	
カード会員データには以下のものが含まれます。	**機密認証データには以下のものが含まれます。**
• プライマリアカウント番号（PAN） • カード会員名 • 有効期限 • サービスコード	• フルトラックデータ（磁気ストライプデータまたはチップ上の同等のデータ） • カード検証コード • PIN／PIN ブロック

PCI DSS 要件は、アカウントデータ（カード会員データや機密認証データ）を保存、処理、または伝送する環境を持つ事業体、およびカード会員データ環境（CDE）のセキュリティに影響を与える可能性がある環境を持つ事業体に適用されます。PCI DSS 要件の一部は、アカウントデータを保存、処理、または伝送しない環境を持つ事業体（たとえば、カード会員データ環境（CDE） の支払業務または管理を外部に

委託している事業体）にも適用される場合があります[1]。決済環境または決済業務を第三者にアウトソースする事業体は、適用される PCI DSS 要件に従ってアカウントデータが第三者によって保護されることに対する責任を負います。

プライマリアカウント番号（PAN）は、カード会員データを定義する要素です。したがって、アカウントデータという用語には、完全な PAN、PAN と共に存在するカード会員データのその他の要素、および機密認証データの要素 が含まれます。

カード会員名、サービスコード、有効期限が PAN と共に保存、処理、または伝送される場合、またはその他の方法でカード会員データ環境（CDE） に存在する場合、カード会員データに適用される PCI DSS 要件に従って保護される必要があります。

事業体が PAN を保存、処理、または伝送する場合は、カード会員データ環境（CDE） が存在するため PCI DSS 要件が適用されます。ただし、すべての要件が適用されるとは限りません。たとえば、事業体が PAN を保存しない場合、要件 3 の保存された PAN の保護に関する要件は、その事業体には適用されません。

事業体が PAN を保存、処理、または伝送しない場合でも、一部の PCI DSS 要件が適用される場合があります。以下の点を考慮してください。

- 事業体が機密認証データ（SAD） を保管する場合、要件 3 の機密認証データ（SAD）の保管に関連する要件が適用されます。
- 事業体が第三者のサービスプロバイダに依頼して、PAN の保存、処理、または伝送を委託する場合、要件 12 のサービスプロバイダの管理に関連する要件が適用されます。
- 事業体のインフラのセキュリティがカード会員データの処理方法に影響することから事業体が カード会員データ環境（CDE） のセキュリティに影響を与える可能性がある場合（例：決済フォームや決済ページの生成を制御するウェブサーバの経由）、一部の要件が適用されます。
- カード会員データが物理メディア（たとえば紙）上にのみ存在する場合は、要件 9 の物理メディアのセキュリティと廃棄に関連する要件が適用されます。

[1]コンプライアンスプログラムを管理する組織（ペイメントブランドやアクワイアラなど）に従い、詳細は各組織にお問い合わせください。

- インシデント対応計画に関する要件はすべての事業体に適用されます。本要件では、カード会員データの機密性が侵害された疑いがある場合、または実際に侵害された場合に従うべき手順があることを確認します。

PCI DSS におけるアカウントデータ、機密認証データ、カード会員データ、プライマリアカウント番号の使用

PCI DSS には、アカウントデータ、カード会員データ、機密認証データについて具体的に言及した要件が含まれています。これらのデータの種類はそれぞれ異なるものであり、用語に互換性がないことに注意してください。要件内ではアカウントデータ、カード会員データ、機密認証データに対してそれぞれ具体的な目的を持ち言及しています。各要件は、要件内で言及された特定のデータタイプのみに適用されます。

アカウントデータの要素および保存要件

表 3 は、カード会員データおよび機密認証データの構成要素と、各データ要素の保存が許可されているか、あるいは禁止されているか、保存時に各データ要素を読み取り不能にする必要があるか（例えば強力な暗号化を使用するなど）を示しています。この表は完全なものではありませんが、各データ要素に適用されるさまざまな種類の要件を示しています。

表 3。アカウントデータの構成要素保存要件

		データ要素	保存要件	保存されたデータを読み取り不能にする必要があるか
アカウントデータ	カード会員情報	プライマリアカウント番号（PAN）	要件 3.2 に従い最小限の保存を行う。	要件 3.5 に従い読み取り不能とする必要がある。
		カード会員名	要件 3.2 に従い最小限の保存を行う。[2]	いいえ
		サービスコード		
		有効期限		
	機密認証データ	フルトラックデータ	要件 3.3.1 に従い承認後は保存できない。[3]	要件 3.3.2 に従い承認前は強力な暗号化で読み取り不能とする必要がある。
		カード検証コード		
		PIN／PIN ブロック		

PAN がカード会員データの他の要素と共に保存される場合、PCI DSS 要件 3.5.1 に従って PAN のみを読み取り不能にする必要があります。承認後の機密認証データは、暗号化されていても保存してはなりません。これは、PAN が存在しない環境にも適用されます。

[2]ただし、イシュアおよびイシュアサービス会社が許可された場合を除きます。

[3] イシュアおよびイシュアサービス会社に対する要件は、要件 3.3.3 にて別途定めています。

3 PCI DSS と PCI SSC ソフトウェア基準の関係

PCI SSC は、ペイメントアプリケーションデータセキュリティ基準（PA-DSS）およびセキュリティソフトウェア基準とセキュア SLC 基準で構成されるセキュリティソフトウェアフレームワーク（SSF）により、カード会員データ環境（CDE）内での安全なペイメントソフトウェアの使用をサポートしています。PCI SSC の検証を受けてリストアップされたソフトウェアは、安全な手法を使用して開発されたものであり、ソフトウェアのセキュリティ要件に適合していることが保証されています。

PCI SSC セキュアソフトウェアプログラムには、該当する PCI SSC ソフトウェア基準を満たすことが検証されたペイメントソフトウェアおよびソフトウェアベンダのリストが含まれています。

- **認定ソフトウェア**：PCI SSC ウェブサイトに PA-DSS 検証済みのペイメントアプリケーション または セキュリティソフトウェア基準で検証済みのソフトウェア として掲載されているペイメントソフトウェアは、当該ソフトウェアが基準内のセキュリティ要件を満たしていることが資格を有する評価者によって検証されています。これらの基準におけるセキュリティ要件は、決済取引とアカウントデータの整合性と機密性を保護することに重点を置いています。
- **認定ソフトウェアベンダ**：セキュア SLC 基準は、ソフトウェアのライフサイクル全体を通じて安全なソフトウェア開発手法を統合するために、ソフトウェアベンダに対するセキュリティ要件を定義しています。セキュア SLC 基準を満たしていると検証されたソフトウェアベンダは、セキュア SLC 基準認定ベンダとして PCI SSC のウェブ サイトに掲載されます。

注意：PA-DSS および関連プログラムは 2022 年 10 月に廃止される予定です。PA-DSS 検証済みアプリケーションの有効期限については は、PCI SSC の検証済みペイメントアプリケーションのリストを参照してください。有効期限を過ぎたアプリケーションは、「既存のデプロイ済み環境でのみ使用可」として表示されます。 有効期限が切れた PA-DSS アプリケーションの使用を継続できるかどうかは、コンプライアンスプログラムを管理する組織（ペイメントブランドやアクワイアラなど）の判断によりますので、詳細は各組織にお問い合わせください。

SSF および PA-DSS の詳細については、それぞれのプログラムガイドを参照してください（www.pcisecuritystandards.org)。

アカウントデータを保存、処理、または伝送するソフトウェア、あるいはアカウントデータまたはカード会員データ環境（CDE） のセキュリティに影響を与える可能性のあるソフトウェアはすべて、事業体の PCI DSS 評価の対象となります。検証済みのペイメントソフトウェアの使用は事業体のカード会員データ環境（CDE） のセキュリティをサポートしますが、ソフトウェアを使用することによって事業体の PCI

DSS 準拠が保証されるわけではありません。事業体が PCI DSS 評価を行うためには、該当する PCI DSS 要件を満たすようにソフトウェアが適切に構成され、安全に実装されていることを検証する必要があります。さらに、PCI SSC のリストに掲載されたペイメントソフトウェアがカスタマイズされている場合、そのソフトウェアが検証時のバージョンと仕様が異なる可能性があるため、PCI DSS 評価の際にさらに詳細なレビューが必要になります。

セキュリティの脅威は常に進化しているため、ベンダのサポートが終了したソフトウェア（たとえば、ベンダが「サポート期限切れ」と認定したもの）は、サポートされるバージョンと同じレベルのセキュリティが提供されない可能性があります。事業体は、ソフトウェアを最新の状態に保ち、利用可能な最新のソフトウェアバージョンに更新することを原則としてください。ソフトウェアを独自に開発する事業体は、PCI SSC のソフトウェアセキュリティ基準を参照し、その要件 を開発環境で使用するベストプラクティスとして考慮してください。PCI DSS に準拠した環境に実装された安全なペイメントソフトウェアは、アカウントデータの漏洩や不正行為につながるセキュリティ侵害の可能性を最小限に抑えるのに役立ちます。個社開発ソフトウェアおよびカスタムソフトウェアを参照してください。

ペイメントソフトウェアベンダに対する **PCI DSS** の適用性

ベンダがアカウントデータを保存、処理、または伝送するペイメントサービスプロバイダである場合、または顧客環境へのリモートアクセスを通じて顧客のアカウントデータにアクセスする場合、PCI DSS がペイメントソフトウェアベンダに適用される場合があります。PCI DSS が適用されるソフトウェアベンダには、ペイメントサービスを提供するベンダのほか、クラウド環境におけるペイメント端末、SaaS、クラウド環境における電子商取引、その他のクラウドペイメントサービスを提供するクラウドサービスプロバイダが含まれます。

個社開発ソフトウェアおよびカスタムソフトウェア

アカウントデータを保存、処理、または伝送する、あるいはアカウントデータまたはカード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるすべての個社開発ソフトウェアおよびカスタムソフトウェアは、事業体の PCI DSS 評価の範囲に含まれます。

PCI SSC のソフトウェアセキュリティフレームワーク基準（セキュリティソフトウェア基準 またはセキュア SLC 基準のいずれか）に準拠して開発および保守されている個社開発ソフトウェアおよびカスタムソフトウェアは、PCI DSS 要件 6 を満たす上で事業体をサポートします。

詳細については、付録 F を参照してください。

注意：PCI DSS 要件 6 は、PCI SSC のソフトウェアセキュリティフレームワーク基準のいずれかに従って開発および保守されていない個社開発ソフトウェアおよびカスタムソフトウェアに全面的に適用されます。アカウントデータまたはカード会員データ環境（CDE）のセキュリティに影響を与える可能性のある個社開発またはカスタムソフトウェアの開発にソフトウェアベンダを使用する事業体は、それらのソフトウェアベンダが PCI DSS 要件 6 に従ってソフトウェアを開発することに対する責任があります。

4 PCI DSS 要件の適用範囲

PCI DSS 要件は、以下に適用されます。

- カード会員データ環境（CDE）

  カード会員データ環境（CDE）は、次のもので構成されます。

  – カード会員データや機密認証データを保存、処理、および伝送するシステムコンポーネント、人、およびプロセス、

  および／または

  – カード会員データ(CHD)／機密認証データ（SAD） を保存、処理、または伝送しないが、カード会員データ(CHD)／機密認証データ（SAD） を保存、処理、または伝送するシステムコンポーネントに無制限の接続性を持つシステムコンポーネント。

および

- カード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるシステムコンポーネント、人、プロセス。[4]

「システムコンポーネント」には、ネットワークデバイス、サーバ、コンピューティングデバイス、仮想コンポーネント、クラウドコンポーネント、およびソフトウェアが含まれます。システムコンポーネントの例としては、以下のものが挙げられますが、これらに限定されるものではありません。

- アカウントデータを保存、処理、または伝送するシステム（たとえば、決済端末、認証システム、クリアリングシステム、決済ミドルウェアシステム、決済バックオフィスシステム、ショッピングカートおよびストアフロントシステム、決済ゲートウェイ／スイッチシステム、不正監視システムなど）。セキュリティサービスを提供するシステム（例えば、認証サーバ、アクセスコントロールサーバ、セキュリティ情報およびイベント管理（SIEM）システム、物理セキュリティシステム（例えば、バッジアクセスまたは CCTV）、多要素認証システム、アンチマルウェアシステムなど）。

---

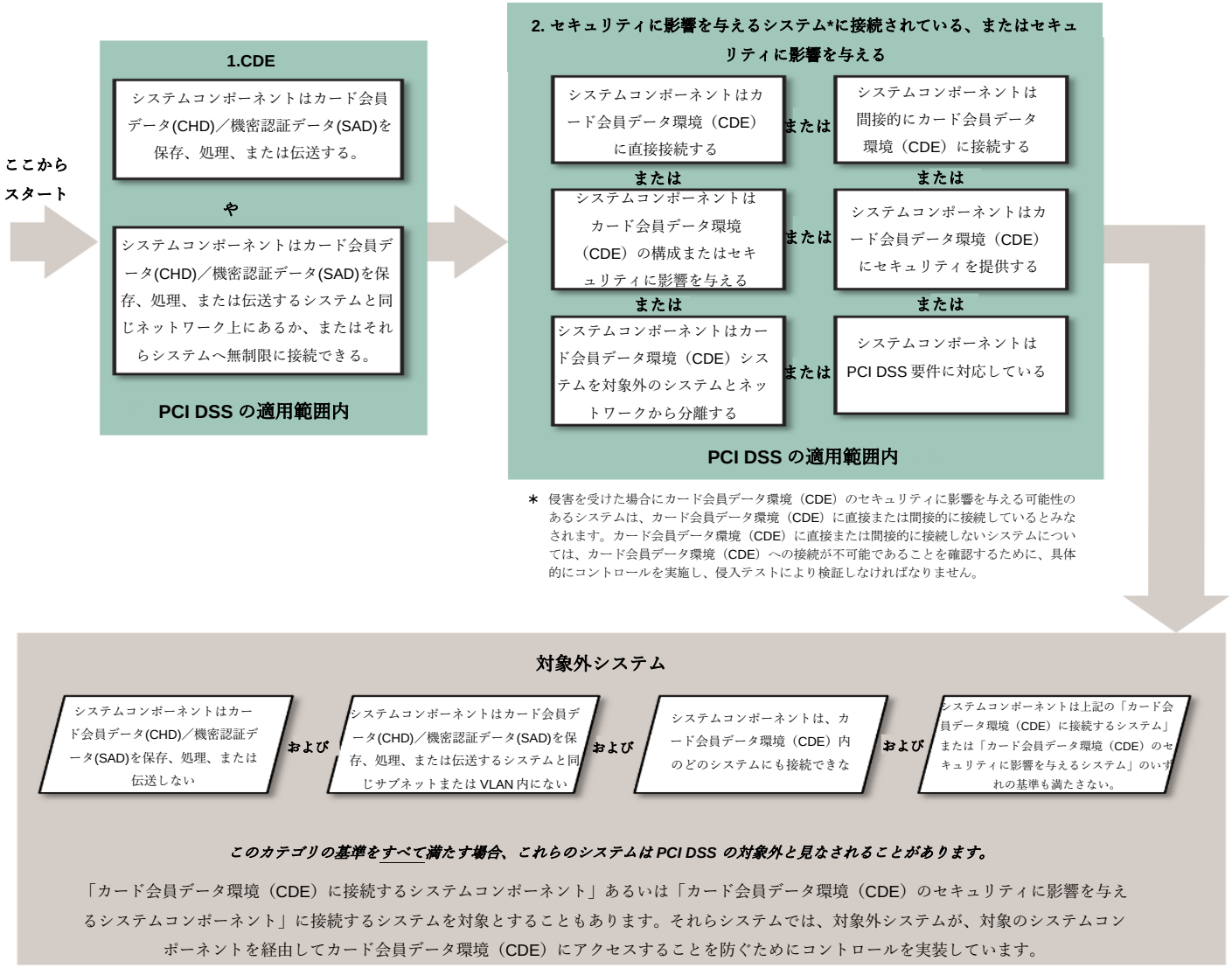
[4] その他のガイダンスについては、*情報補足*を参照してください。PCI SSC の Web サイトにある *PCI DSS の適用範囲とネットワークセグメンテーションのためのガイダンス* をご覧ください。

- セグメンテーションを促進するシステム（例えば、内部ネットワークのセキュリティコントロール）。
- アカウントデータまたはカード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるシステム（例えば、名前解決、または電子商取引（ウェブ）リダイレクトサーバ）。
- 仮想マシン、仮想スイッチ／ルーター、仮想アプライアンス、仮想アプリケーション／デスクトップ、ハイパーバイザーなどの仮想化コンポーネント。
- クラウドインフラストラクチャとコンポーネント（外部とオンプレミスの両方）。コンテナまたはイメージのインスタンス化、仮想プライベートクラウド、クラウドベースのアイデンティティとアクセス管理、オンプレミスまたはクラウドにあるカード会員データ環境（CDE）、コンテナ化アプリケーションとのサービスメッシュ、コンテナオーケストレーションツールを含みます。
- ネットワークコンポーネント。ネットワークセキュリティコントロール、スイッチ、ルーター、VoIP ネットワークデバイス、無線アクセスポイント、ネットワークアプライアンス、その他のセキュリティアプライアンスを含むが、これらに限定されるものではありません。
- 各種サーバ（ウェブ 、アプリケーション、データベース、認証、メール、プロキシ、ネットワークタイムプロトコル（NTP）、ドメインネームシステム（DNS）などを含みますが、これらに限定されるものではありません）。
- コンピュータ、ラップトップ、ワークステーション、管理用ワークステーション、タブレット、モバイルデバイスなどのエンドユーザデバイス。
- プリンター、およびスキャン、印刷、ファックスを行う多機能デバイス。
- あらゆる形式のアカウントデータの保存（例えば、紙、データファイル、音声ファイル、画像、ビデオ録画など）。
- アプリケーション、ソフトウェア、ソフトウェアコンポーネント、サーバレスアプリケーション（購入、サブスクライブ（SaaS など）、個社開発ソフトウェアおよびカスタムソフトウェアのすべてを含み、内部および外部（インターネットなど）アプリケーションを含む）。
- ソフトウェアの構成管理を実装するツール、コードリポジトリ、およびシステム。

  また、カード会員データ環境（CDE）またはカード会員データ環境（CDE）に影響を与えるシステムに対してオブジェクトをデプロイするためのツール、コードリポジトリ、およびシステム。

図 1 は、システムコンポーネントに対して PCI DSS の適用範囲を設定する際に考慮すべき事項を示しています。

図 1。PCI DSS の適用範囲を理解する



年次 **PCI DSS** 適用範囲確認

PCI DSS 評価準備の最初のステップは、事業体が評価範囲を正確に決定することです。評価事業体は、PCI DSS 要件 12.5.2 に従って、アカウントデータのすべての場所とフローを特定し、カード会員データ環境（CDE）に接続している、または侵害された場合にカード会員データ環境（CDE）に影響を与える可能性のあるすべてのシステム（認証サーバ、リモートアクセスサーバ、ログサーバなど）を特定し、PCI DSS 適用範囲に含めることで、PCI DSS の正確性を確認しなければなりません。バックアップ／リカバリサイトやフェイルオーバーシステムなど、すべてのタイプのシステムと拠点を適用範囲適用範囲決定プロセスで考慮しなければなりません。

事業体が PCI DSS 適用範囲の正確性を確認するための最小限の手順は、PCI DSS 要件 12.5.2 に規定されています。事業体は、PCI DSS 適用範囲がどのように決定されたかを示す文書を保持することが期待されます。この文書は、評価者のレビューのため、および事業体の次回の PCI DSS 適用範囲の確認アクティビティで参照するために保持されます。評価者は、PCI DSS 評価ごとに、事業体が評価の範囲を正確に定義し、文書化したことを検証します。

***注意**：PCI DSS 適用範囲の年次確認は、PCI DSS 要件 12.5.2 で定義されており、事業体が実施するアクティビティです。このアクティビティは、評価者が実施する適用範囲確認と同じではなく、またそれに取って代わることを意図していません。*

セグメンテーション

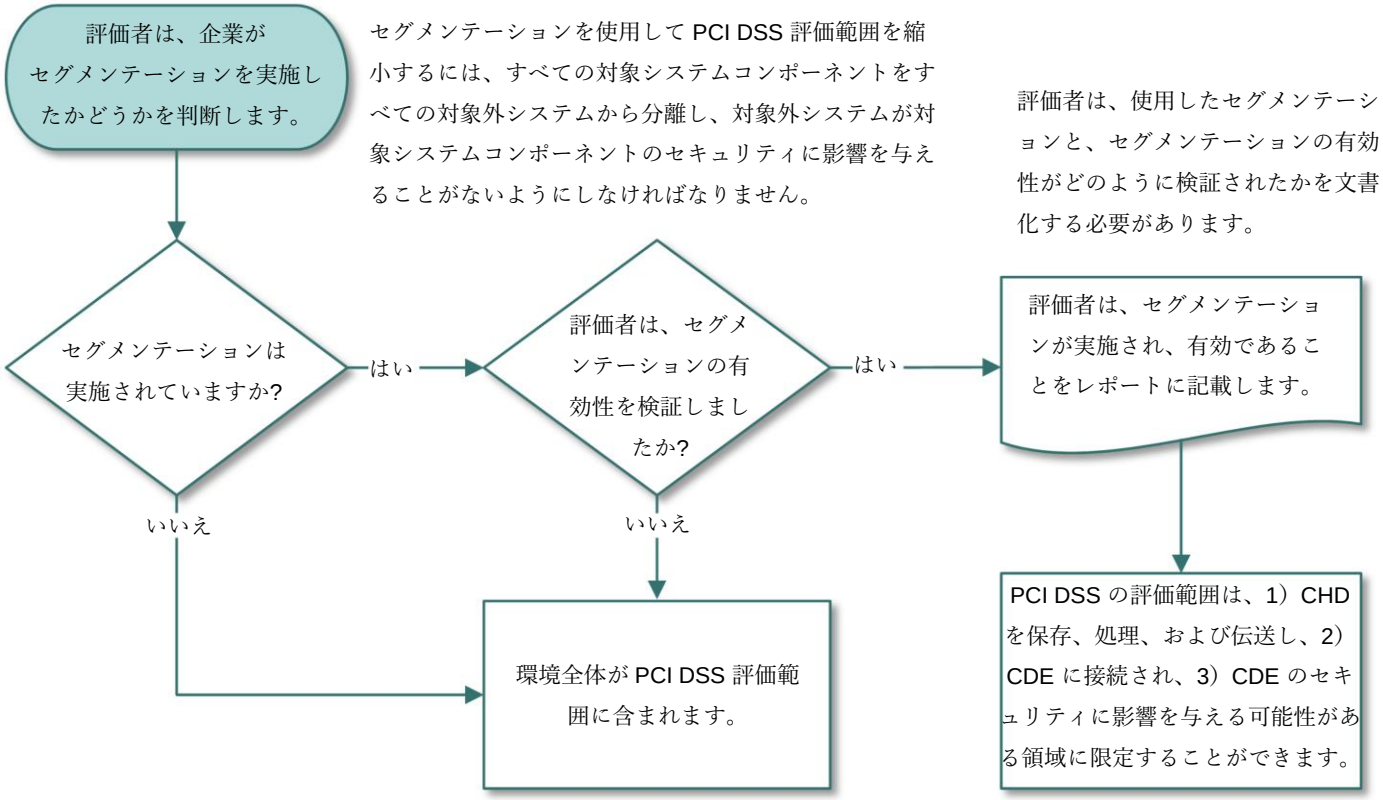
- カード会員データ環境（CDE） を事業体のネットワークの残りの部分からセグメンテーション（または分離）することは、PCI DSS の要件ではありません。しかし、以下を低減する可能性がある方法として強く推奨します。
- PCI DSS 評価範囲
- PCI DSS 評価のコスト
- PCI DSS コントロールの実装と維持にかかるコストと難易度
- ペイメントカードのアカウントデータを扱う事業体のリスク（データをより少ない場所、より管理を強化した場所に統合することによってリスクを低減します。）

適切なセグメンテーションがなければ（「フラットネットワーク」と呼ばれることもある）、ネットワーク全体が PCI DSS の評価範囲になります。セグメンテーションは、適切に構成された内部ネットワークセキュリティコントロール、強力なアクセスコントロールリストを備えたルータ、またはネットワークの特定のセグメントへのアクセスを制限するその他のテクノロジなど、多くの物理的または論理的な方法を使用して実現できます。PCI DSS の適用範囲外と見なされるには、システムコンポーネントが カード会員データ環境（CDE） から適切にセグメント化（分離）され、適用範囲外のシステムコンポーネントが侵害されても カード会員データ環境（CDE） のセキュリティに影響を与カード会員データ環境（CDE） の範囲を縮小するための重要な前提条件は、アカウントデータの保存、処理、および伝送に 関連するビジネスニーズとプロセスを明確に理解することです。不要なデータを削除し、必要なデータを統合することで、口座データをできるだけ少ない場所に制限するためには、長年にわたるビジネスプラクティスのリエンジニアリングが必要になる場合があります。

アカウントデータの流れをデータフロー図によって文書化することは、アカウントデータがどのように事業体に入ってくるのか、事業体内のどこにあるのか、事業体内の様々なシステムをどのように経由しているのかを事業体が完全に理解するのに役立ちます。また、データフロー図は、アカウントデータが保存、処理、および伝送されるすべての場所を示しています。この情報は、セグメンテーションを実施する事業体をサポートし、カード会員データ環境（CDE）を範囲外のネットワークから分離するためにセグメンテーションが使用されていることを確認することもできます。

セグメンテーションを使用して PCI DSS 評価範囲を縮小する場合、評価者は、図 2 に示すように、評価範囲を縮小するためにセグメンテーションが適切であることを確認する必要があります。高度なレベルでは、適切なセグメンテーションによって、アカウントデータを保存、処理、または伝送するシステムとそうでないシステムが分離されます。しかし、特定のセグメンテーションが適切であるかどうかは、ネットワークの構成、導入されている技術、導入の可能性がある他のコントロールなど、いくつかの要因によって大きく変化します。

図 2。セグメンテーションと PCI DSS 適用範囲への影響



ワイヤレス

アカウントデータの保存、処理、伝送にワイヤレステクノロジを使用する場合（ワイヤレス POS デバイスなど）、またはワイヤレスローカルエリアネットワーク（WLAN）がカード会員データ環境（CDE）の一部であるかカード会員データ環境（CDE）に接続されている場合、ワイヤレス環境のセキュリティに関する PCI DSS 要件とテスト手順が適用され、実行しなければなりません。

カード会員データ環境（CDE） 内でワイヤレスが使用されておらず、事業体がその環境内でのワイヤレステクノロジの使用を禁止するポリシーを持っている場合でも、PCI DSS 要件 11.2.1 に従って不正ワイヤレス検出を実行しなければなりません。これは、ワイヤレスアクセスポイントは簡単にネットワークに接続でき、その存在を検出することが困難であり、未承認のワイヤレスデバイスによってリスクが増大するためです。

ワイヤレステクノロジを導入する前に、事業体はリスクに対するテクノロジの必要性を慎重に評価しなければなりません。ワイヤレステクノロジの導入は、機密性のないデータ伝送のためにのみ行うことを検討します。

暗号化されたカード会員データおよび **PCI DSS** 適用範囲への影響

強力な暗号を使用したカード会員データの暗号化は、PCI DSS 要件 3.5 に従ってデータを読み取り不能にするための方法として許容されます。ただし、暗号化だけでは一般に、カード会員データを PCI DSS の適用範囲外にすることはできず、その環境における PCI DSS 準拠の必要性がなくなるわけではありません。カード会員データが存在するため、その事業体の環境は依然として PCI DSS の適用範囲内にあります。たとえば、カードを提示する加盟店では、取引を完了するためにペイメントカードに物理的にアクセスし、カード会員データを含む紙のレポートまたは領収書が存在する場合もあります。同様に、通信販売／電話注文や電子商取引などのカードを提示しない加盟店では、PCI DSS に従って評価および保護されたチャネルを介してペイメントカードの詳細情報が提供されます。

PCI DSS 評価範囲には、以下のものがあります。

- カード会員データの暗号化や復号化を実行するシステム、および鍵管理機能を実行するシステム。
- 暗号化、復号化および鍵管理プロセスから分離されていない暗号化されたカード会員データ。
- 暗号化されたカード会員データで、復号鍵と同じシステムまたはメディアに存在するもの。
- 暗号化されたカード会員データで、復号鍵と同じ環境下に存在するもの。
- 暗号化されたカード会員データで、復号鍵へのアクセスも持つ事業体がアクセスできるもの。

注：PCI に準拠した P2PE ソリューションを使用すると、加盟店のカード会員データ環境に適用される PCI DSS 要件の数を大幅に削減することができます。ただし、加盟店の環境における PCI DSS の適用を完全に排除するものではありません。

暗号化されたカード会員データおよびサードパーティサービスプロバイダの **PCI DSS** 適用範囲への影響

サードパーティサービスプロバイダ（TPSP）が、他の事業体によって暗号化データのみを受信、保存し、データを復号化する能力を持たない場合、TPSP は、一定の条件を満たせば、暗号化データを適用範囲外とみなすことが可能です。これは、一般に、データを復号化する能力、または暗号化データのセキュリティに影響を与える能力を持つ事業体がデータに対する責任を持つためです。どの当事者がどの PCI DSS コントロールに責任を持つか決定するためには、誰が復号鍵へのアクセス権を持つか、各当事者の役割は何か、当事者間の合意など、複数の要因が考慮されます。TPSP と暗号化データを提供する事業体の両方が、どの事業体がどのセキュリティコントロールに 責任を持つかを理解できるように、責任を明確に定義して文書化しなければなりません。

例として、ストレージサービスを提供する TPSP が、バックアップ目的で顧客から提供された暗号化されたカード会員データを受領し、保管するとします。この TPSP は、暗号鍵または復号鍵にアクセスすることはできず、また、顧客のために鍵管理を行うこともありません。TPSP は、PCI DSS の適用範囲を決定する際に、そのような暗号化データを除外することができます。ただし、TPSP は、顧客とのサービス契約の一環として、暗号化データストレージへのアクセスコントロールに対する責任を負います。

PCI DSS 要件に従って暗号化データおよび暗号鍵が保護されていることを確認する責任は、多くの場合、事業体間で共有されます。上記の例では、顧客は、どの担当者がストレージメディアにアクセスする権限を有するかを決定する。また、ストレージ施設は、顧客によって許可された者のみがストレージメディアにアクセスするように、物理的、論理的アクセスコントロールを管理する責任を有します。TPSP に適用される PCI DSS 要件は、提供されるサービスおよび両当事者間の契約によって異なります。ストレージサービスを提供する TPSP の例では、TPSP が提供する物理的および論理的なアクセスコントロールを少なくとも年 1 回レビューする必要があります。このレビューは、加盟店の PCI DSS 評価の一部として実施されるか、または適切な証跡を加盟店に提供し、TPSP がレビューを実施、コントロールを検証することができます。「適切な証跡」については、顧客の PCI DSS 要件を満たす TPSP サービスの PCI DSS 準拠を検証するための TPSP のオプションを参照してください。

別の例として、他の事業体にルーティングする目的で暗号化されたカード会員データのみを受信し、データまたは暗号鍵にアクセスしない TPSP は、その暗号化データに対して PCI DSS 上の責任を持たない場合があります。このシナリオでは、TPSP がセキュリティサービスまたはアクセスコントロールを提供していない場合、TPSP は公共または信頼できないネットワークと同じと見なされ、TPSP のネットワークを通じてアカウントデータを送受信する事業体が、送信されるデータを保護するために PCI DSS コントロールを適用する責任を負うことになります。

サードパーティサービスプロバイダの使用

ある事業体（このセクションでは「顧客」）は、顧客に代わってアカウントデータを保存、処理、伝送するため、または適用範囲内のシステムコンポーネントを管理するために、サードパーティサービスプロバイダ（TPSP）を使用することを選択する場合があります。TPSP の使用は、顧客の カード会員データ環境（CDE） のセキュリティに影響を与える可能性があります。

注：*PCI DSS 準拠の TPSP を使用することによって、顧客が PCI DSS に準拠するわけではなく、また、顧客自身の PCI DSS 準拠に対する責任がなくなるわけではありません。顧客が TPSP を使用してすべてのアカウントデータ機能を満たす場合でも、コンプライアンスプログラムを管理する組織（ペイメントブランドやアクワイアラなど）の要求に応じて、顧客自身のコンプライアンスを確認する責任は残ります。顧客は、顧客は、要件について関連組織に問い合わせなければなりません。*

TPSP の使用と、PCI DSS 要件 12.8 を満たす顧客への影響

顧客のカード会員データ環境（CDE）内に存在する機能、あるいは関連する機能の実現のために一つ以上の TPSP を使用するシナリオは多数あります。TPSP を使用するすべてのシナリオにおいて、顧客は要件 12.8 に従って、以下の TPSP を含むすべての TPSP の PCI DSS 準拠状況を管理および監督する必要があります。

- 顧客のカード会員データ環境（CDE）にアクセスできる TPSP、
- 顧客に代わって適用範囲内のシステムコンポーネントを管理する TPSP、および／または、
- 顧客のカード会員データ環境（CDE）のセキュリティに影響を与えることができる TPSP。

- 要件 12.8 に従って TPSP を管理することは、デューデリジェンスの実施、適切な契約の締結、顧客に適用される要件と TPSP に適用される要件の識別、および少なくとも年 1 回の TPSP の準拠ステータスの監視を含んでいます。
- 要件 12.8 は、顧客の TPSP が PCI DSS に準拠しなければならないとは規定していませんが、要件で規定され ているように、顧客が TPSP の準拠ステータスを監視することのみを規定しています。したがって、顧客が要件 12.8 を満たすために、TPSP が PCI DSS に準拠する必要はありません。

*顧客の **PCI DSS 要件**を満たすサービスに **TPSP** を使用した場合の影響*

TPSP が顧客の代わりに PCI DSS 要件を満たすサービスを提供する場合、またはそのサービスが顧客のカード会員データ環境（CDE）のセキュリティに影響を与える可能性がある場合、それらの要件は顧客の評価対象となり、そのサービスの準拠が顧客の PCI DSS 準拠に影響を与えます。TPSP は、該当する PCI DSS 要件を満たしていることを、顧客のために証明しなければなりません。たとえば、ある事業体がネットワークセキュリティコントロールの管理を TPSP に依頼する場合、TPSP が PCI DSS 要件 1 の該当する要件を満たしていることを示す証跡を提供しなければ、顧客は要件を満たすことができません。別の例として、顧客に代わってカード会員データのバックアップを保存する TPSP は、アクセスコントロール、物理セキュリティなどに関連する適用別の例として、顧客に代わってカード会員データ要件を満たす必要があります。TPSP が関連要件を満たす場合、顧客はこれらの要件を満たしているとみなすことができます。

***TPSP** 顧客と **TPSP** の間の責任を理解することの重要性*

顧客と TPSP は、以下の事項を明確にし、理解する必要があります。

- TPSP の PCI DSS 評価範囲に含まれるサービスおよびシステムコンポーネント。
- TPSP の PCI DSS 評価対象となる PCI DSS 要件および下位要件。
- TPSP の顧客が自らの責任において PCI DSS 評価に含める要件、および
- TPSP と顧客との間で責任が共有される PCI DSS 要件。

たとえば、クラウドプロバイダは、四半期ごとの脆弱性スキャン プロセスの一環として自社の IP アドレスのどれをスキャンし、どの IP アドレスを顧客の責任でスキャンするのかを明確に定義する必要があります。

要件 12.9.2 に従い、TPSP は、顧客に提供するサービスに関連する TPSP の PCI DSS 準拠ステータス、どの PCI DSS 要件が TPSP の責任であり、どの PCI DSS 要件が顧客の責任であり、また、顧客と TPSP 間にどのような責任があるかについて、顧客からの要求に応じてサポートしなければなりません。*PCI DSS v4.0 を理解するためのヒントとツール*を参照し、TPSP と顧客の間でどのように責任を共有するかを文書化し明確にするために使用できる責任マトリックステンプレートを活用してください。

*顧客の **PCI DSS** 要件を満たす **TPSP** サービスの **PCI DSS** 準拠を検証するための **TPSP** のオプション*

TPSP は、コンプライアンスプログラムを管理する組織（ペイメントブランドやアクワイアラなど）からの要求に応じて、PCI DSS 準拠を証明する責任を負います。 TPSP は、要件について関連組織に問い合わせる必要があります。

TPSP が顧客の PCI DSS 要件を満たす、または満たすサポートをするサービスを提供する場合、または顧客の カード会員データ環境（CDE） のセキュリティに影響を与える可能性がある場合、これらの要件は顧客の PCI DSS 評価範囲に含まれます。本シナリオで TPSP が準拠を検証するために、2 つのオプションがあります。

- **年次評価**：TPSP が年次の PCI DSS 評価を受けて、TPSP が該当する PCI DSS 要件を満たしていることを示す証跡を顧客に提供する、または 。
- **複数回のオンデマンド評価**：TPSP が毎年の PCI DSS 評価を受けていない場合、顧客の要求に応じて評価を受けるか、または顧客の各 PCI DSS 評価に参加し、各レビューの結果を顧客に提供しなければならない。

TPSP が独自の PCI DSS 評価を受けている場合、TPSP の PCI DSS 評価が、顧客の利用サービスも含んでおり、関連する PCI DSS 要件が検証され、満たしていることが確認できる十分な証跡を提供することが期待されます。プロバイダが PCI DSS 準拠証明書（AOC）を所有している場合、TPSP は要求に応じて AOC を顧客に提供することが期待されています。また、顧客は TPSP の PCI DSS 準拠報告書（ROC）の関連するセクションを要求することもできます。ROC は、機密情報を保護するために改訂される場合があります。

TPSP が独自の PCI DSS 評価を受けておらず、AOC を保持していない場合、 TPSP が PCI DSS 要件を満たしていることを顧客（またはその評価者）が確認できるように、該当する PCI DSS 要件に関連する証跡を提供することが期待されます。

PCI DSS 準拠サービスプロバイダのペイメントブランドリストにおける TPSP の掲載

要件 12.8 に従って TPSP の準拠ステータスを監視している顧客にとって、顧客の利用サービスが TPSP の PCI DSS 評価の対象であることが当該リストから明らかである場合、ペイメントブランドの PCI DSS 準拠サービスプロバイダ一覧に掲載されていれば、TPSP の準拠ステータスの***十分な証跡となる***場合があります。リストから明らかでない場合、顧客は TPSP の PCI DSS 準拠ステータスを確認できる他の確認書を入手する必要があります。

顧客が TPSP の準拠済み要件に関する証跡を求めている場合、あるいは TPSP から提供されるサービスが顧客のカード会員データ環境（CDE）のセキュリティに影響を与える場合、PCI DSS 準拠済みサービスプロバイダのリストへの掲載は、TPSP が要件を満たしていることを示す十分な証跡とはなりません。。TPSP が PCI DSS AOC を保有している場合、必要に応じて AOC を顧客に提供することで、自らが要件を満たしていることを証明できます。

5 PCI DSS を日常業務のプロセスに導入するためのベストプラクティス

セキュリティ戦略の一環として日常業務プロセス、別名 BAU を実施する事業体は、データや環境を保護するために実装されたセキュリティコントロールが、通常の業務として正しく実施され機能し続けていることを確認するための措置を講じています。

PCI DSS 要件の中には、セキュリティコントロールを監視してその有効性を継続的に確認することにより、BAU プロセスとして機能するものがあります。事業体が行うこの監視により、PCI DSS 評価間に準拠環境を維持できるという合理的な保証を提供することができます。現在、本基準内にはいくつかの BAU 要件が定義されていますが、事業体は可能な限り、その事業体と環境に特化した BAU プロセスを追加する必要があります。BAU プロセスは、自動コントロールおよび手動コントロールが期待どおりに機能していることを検証するための方法です。PCI DSS 要件が自動か手動かにかかわらず、BAU プロセスでは異常を検出して警告および報告し、担当者がタイムリーに状況に対処できるようにすることが重要です。

PCI DSS を BAU アクティビティに組み込む方法の例としては、以下のものが挙げられますが、これらに限定されるものではありません。

- PCI DSS 準拠に対する全体的な責任と説明責任を個人またはチームに割り当てます。これには、特定の PCI DSS 準拠プログラムについて経営層が定義した憲章と、経営層へのコミュニケーションを含めることができます。
- セキュリティコントロールの効果を測定するパフォーマンス指標を開発し、ネットワークセキュリティコントロール、侵入検知システム／侵入防止システム（IDS／IPS）、変更検知メカニズム、アンチマルウェアソリューション、アクセスコントロールなどの依存度が高いセキュリティコントロールを継続的に監視して、それらが効果的かつ意図通りに動作していることを確認します。
- ログデータを頻繁にレビューし、監視だけではわからない傾向や挙動を把握します。
- セキュリティコントロールにおけるすべての障害を確実に検知し、迅速に対応します。セキュリティコントロールの障害に対応するプロセスには、以下を含めるべきです。
  - セキュリティコントロールの復旧。
  - 障害の原因特定。
  - セキュリティコントロールの障害時に発生したセキュリティ上の問題の特定と対処。

- 低減策の実施（プロセスやテクニカルコントロールなどにより障害原因の再発防止）。
- 一定期間監視を強化してセキュリティコントロールの監視を再開し、コントロールが効果的に行われていることを確認。

- 環境にセキュリティリスクをもたらす可能性のある変更（例えば、新システムの追加、システムまたはネットワーク構成の変更など）を、変更完了前にレビューし、以下を含むようにします。
  - リスク評価を実施して、PCI DSS 適用範囲への潜在的な影響を判断します（たとえば、カード会員データ環境（CDE）内のシステムと別のシステム間の接続を許可する新しいネットワークセキュリティコントロールルールにより、追加のシステムまたはネットワークが PCI DSS 適用範囲に入る可能性があります）。
  - 変更の影響を受けるシステムおよびネットワークに適用される PCI DSS 要件を特定します（たとえば、新しいシステムが PCI DSS 適用範囲に入る場合、変更検出メカニズム、マルウェア対策ソフトウェア、パッチ、監査ログなど、システム構成基準に従って構成する必要があります。これらの新しいシステムおよびネットワークは、適用範囲内のシステムコンポーネントのインベントリに追加し、四半期ごとの脆弱性スキャンスケジュールに追加する必要があります）。
  - PCI DSS 適用範囲を更新し、必要に応じてセキュリティコントロールを実施します。
  - 実施した変更を反映するために文書を更新します。
- 組織構造の変更（会社の合併や買収など）に伴う PCI DSS 適用範囲および PCI DSS 要件への影響を検討します。
- 外部接続およびサードパーティアクセスを定期的に見直します。
- ソフトウェア開発に第三者を使用している事業体では、それらのソフトウェア開発アクティビティが要件 6 のソフトウェア開発要件に継続して準拠していることを定期的に確認します。
- 定期的なレビューを行い、PCI DSS 要件を継続して満たしていること、および担当者が確立されたプロセスに従っていることを確認します。定期的なレビューは、自己管理または TPSP を使用しているかどうかにかかわらず、小売店やデータセンターを含むすべての施設と場所を対象とする必要があります。例えば、構成基準が適用されたシステム、デフォルトのベンダアカウントとパスワードの削除または無効化、パッチとアンチマルウェアソリューションが最新であること、監査ログのレビューなどを確認するために定期

的なレビューを使用することができます。定期的なレビューの頻度は、PCI DSS に特に記載がない場合、環境の規模および複雑性に応じて事業体が決定する必要があります。

これらのレビューは、PCI DSS 評価に必要なエビデンスが維持されていることを検証するためにも使用することができます。たとえば、監査ログ、脆弱性スキャンレポート、ネットワークセキュリティコントロールルールセットのレビューなどの証跡は、事業体が次回の PCI DSS 評価に向けて準備する際に必要なものです。

- 新たに特定された脅威および組織構造の変更について、外部および内部のすべての影響を受ける当事者とのコミュ ニケーションを確立します。コミュニケーション資料により、脅威の影響、低減策、詳細情報またはエスカレーションのための連絡先を理解することができます。
- ハードウェアおよびソフトウェアテクノロジを少なくとも 12 カ月に 1 回レビューし、ベンダのサポートが継続され、事業体の PCI DSS を含むセキュリティ要件を満たすことができることを確認します。ベンダサポートが終了したテクノロジや事業体のセキュリティ要件を満たせないテクノロジについては、事業体は必要に応じてテクノロジの交換を含む改善計画を作成する必要があります。

注：*本セクションの一部のベストプラクティスは、特定の事業体に対する PCI DSS 要件として含まれています。たとえば、PCI DSS のフル評価を受ける事業体、「サービスプロバイダのみ」の追加要件に対して検証を行うサービスプロバイダ、および付録 A3：指定事業体に対する補足検証 に従って検証を行う必要がある指定事業体などです。*

各事業体は、これらのベストプラクティスを検証する必要がない場合でも（たとえば、自己問診を行っている加盟店）、その環境に導入することを検討する必要があります。

その他のガイダンスについては、PCI SSC ウェブサイトのドキュメントライブラリにある *PCI DSS 準拠を維持するためのベストプラクティス*を参照してください。

6 評価者へ向けて：PCI DSS 評価のためのサンプリング

サンプリングは、テスト対象となる母集団の項目が多い場合、評価プロセスを円滑にするために、PCI DSS を評価する評価者が使用できるオプションのひとつです。

評価者が事業体の PCI DSS 準拠のレビューの一環として対象となる母集団の類似した項目からサンプリングすることは認められますが、事業体が事業体の環境のサンプルだけに PCI DSS 要件を適用することは認められません（たとえば、四半期ごとの脆弱性スキャンの要件はすべてのシステムコンポーネントに適用されます）。同様に、準拠するために PCI DSS 要件のサンプルのみを評価者がレビューすることも認められません。

サンプリングにより、評価者は与えられたサンプリング母数の 100%未満をテストすることができますが、評価者は常に可能な限り完全なレビューを行うように努力する必要があります。評価者は、規模に関係なく完全な母集団を迅速かつ効率的にテストでき、事業体のリソースへの影響が最小限であれば、自動化プロセスまたはその他のメカニズムを使用することが推奨されます。100%のサンプリング母数をテストする自動化プロセスが利用できない場合、サンプリングも同様に容認できるアプローチです。

評価者は、評価対象環境の全体的な範囲、複雑さ、および一貫性、ならびに要件を満たすために事業体が使用するプロセスの性質（自動または手動）を考慮した後、PCI DSS 要件に対する事業体の準拠を評価するために、レビュー対象内から代表となるサンプルを独自に選択することができます。サンプルはレビュー対象内のすべての種類から代表して抽出しなければならず、レビュー対象全体にわたってコントロールが期待どおりに実施されていることを評価者に保証するのに十分な量でなければなりません。要件が定める定期的に行うべき事項をテストする場合（たとえば、毎週、四半期ごと、または定期的に）、評価者は、評価対象全期間を代表するサンプルを選択し、評価期間を通じて要件が満たされたことを合理的に判断できるようにする必要があります。毎年同じ項目のサンプルをテストすると、非サンプル項目の未確認の変化が検出されないままになる可能性があります。評価者は、各評価のためのサンプリングの根拠を再検証し、以前のサンプルセットを考慮する必要があります。各評価において、異なるサンプルを選択しなければなりません。

サンプルの適切な選択は、サンプルとなる対象を調べる際に何を考慮するかによります。例えば、悪質なソフトウェアに冒される可能性があるサーバのアンチマルウェアの有無を判断するには、環境内の全サーバ、特定のオペレーティングシステムを実行する全サーバ、またはメインフレームではない全サーバなどの母集団を決定することにつながる可能性があります。適切なサンプルを選択するには、特定された母集団

の全対象の代表が含まれます。これには、すべてのバージョンを含む特定のオペレーティングシステムを実行しているすべてのサーバ、加えて、母集団の中で異なる機能に使用されているサーバ（ウェブ サーバ、アプリケーションサーバ、データベースサーバなど）が含まれる。

特定の構成項目を検討する場合、母集団を適切に分割し、個別のサンプルグループを特定することができます。例えば、環境内に異なるオペレーティングシステムが存在する場合、オペレーティングシステムの構成設定を検討する際に、すべてのサーバのサンプルは適切でない場合があります。この場合、各オペレーティングシステムの構成が適切に設定されていることを確認するために、各オペレーティングシステムの種類からサンプルを抽出することが適切です。各サンプルセットには、各オペレーティングシステムの種類、バージョン、代表的な機能などを代表するサーバを含めることが望ましいです。

その他のサンプリングの例としては、評価される要件に基づいて、管理者と全従業員のサンプルのように、類似した、または、様々な役割を持つ担当者を選択することが含まれます。

評価者は、サンプルの計画、実施、評価において専門的な判断を行い、事業体が要件を満たしているかどうか、またどのように満たしているかについての結論を支持することが要求されます。評価者のサンプリングにおける目標は、事業体が主張する妥当な根拠となる十分な証跡を入手することです。サンプルを独自に選択する場合、評価者は以下の点を考慮する必要があります。

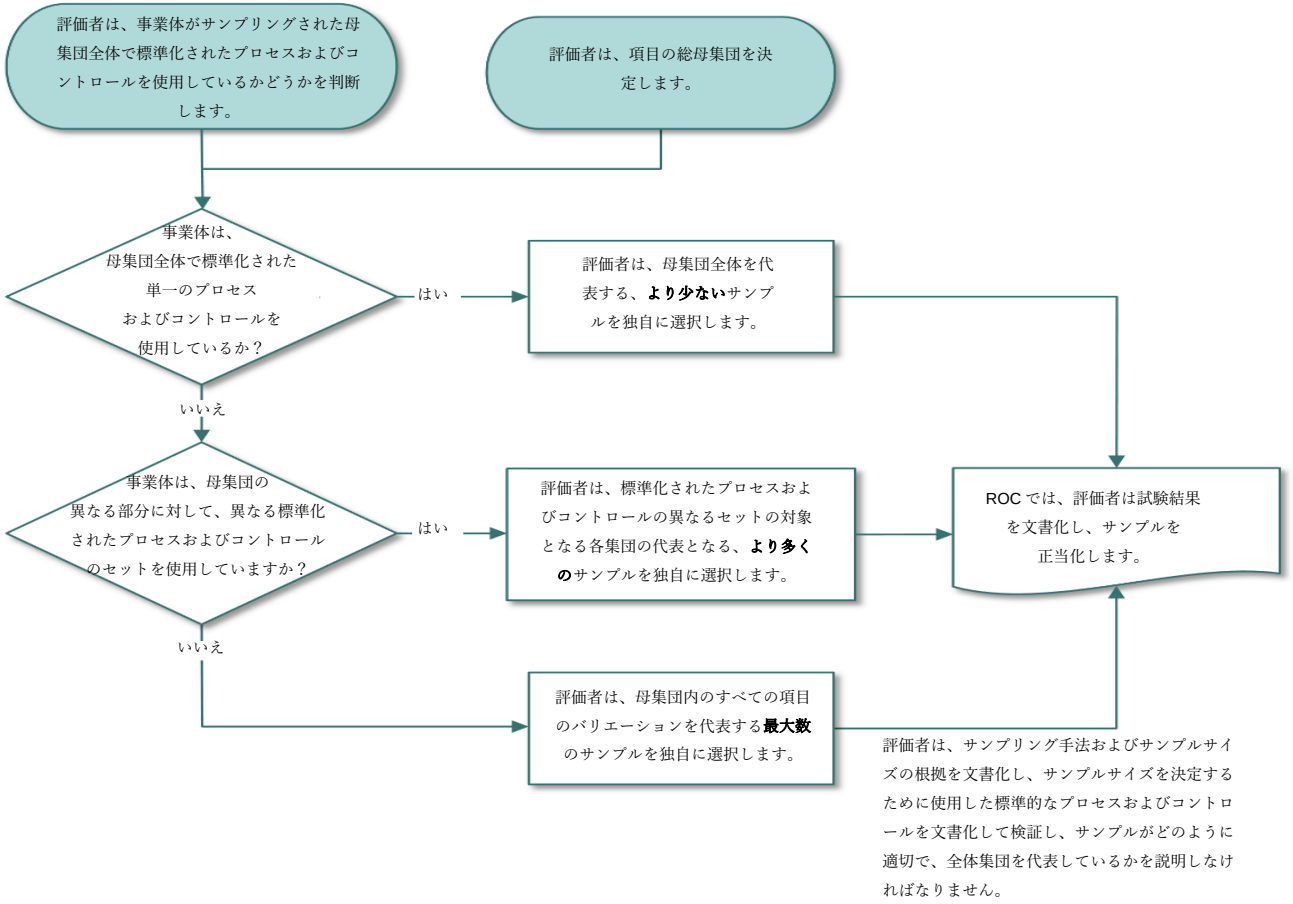
- 評価者は、事業体から影響を受けることなく、完全な母集団からサンプルを選択しなければなりません。
- 事業体が、一貫性を確保し、母集団の各項目に適用される標準的なプロセスおよびコントロールを有している場合には、標準的なプロセス／コントロールを有していない場合よりもサンプルを少なくすることができます。サンプルは、母集団内の項目が母集団内の各項目に適用されている標準化されたプロセスに準拠していることを評価者が合理的に保証するのに十分な量でなければなりません。評価者は、標準化されたコントロールが実施され、効果的に機能していることを検証しなければなりません。
- 事業体が複数の種類の標準化プロセスを導入している場合（例えば、異なる種類の事業施設／システム構成要素について）、サンプルには、それぞれの種類のプロセスの対象となる項目が含まれていなければなりません。例えば、母集団を、異なるプロセスやツールの使用など、評価される要件の一貫性に影響を与える可能性のある特性に基づいて、小集団に分割することができます。その後、各サブ集団からサンプルを選択します。
- 事業体に標準化された PCI DSS プロセス／コントロールがなく、母集団内の各項目が非標準化プロセスで管理されている場合、PCI DSS 要件が母集団内の各項目に適切に適用されていると評価者が保証するには、サンプルをより多くする必要があります。

- システムコンポーネントのサンプルには、使用されているすべてのタイプおよび組み合わせを含める必要があります。事業体が複数のカード会員データ環境（CDE）を持つ場合、サンプルには、適用範囲内のすべてのシステムコンポーネントにわたる母集団を含める必要があります。例えば、アプリケーションをサンプルとする場合、サンプルには、アプリケーションの種類ごとにすべてのバージョンとプラットフォームが含まれていなければなりません。
- サンプルサイズは、与えられた母集団の中に 1 つの項目しかない場合、または評価者が評価された各サンプル母集団についてコントロールがプログラム通りに機能していることを確認した自動コントロールが使用されている場合を除き、常に 1 より多くなければなりません。
- 評価者は、サンプルを選択する根拠として標準化されたプロセスおよびコントロールが実施されていることに依存し、テスト中に標準化されたプロセスおよびコントロールが実施されていない、または効果的に機能していないことが判明した場合は、サンプルサイズを増やして PCI DSS 要件が満たされていることを保証するよう試みなければなりません。

サンプリングが使用される各例について、評価者は次のことを行う必要があります。

- サンプリング手法およびサンプルサイズの根拠を文書化する。
- サンプルサイズの決定に使用した標準化されたプロセスおよびコントロールを検証し、文書化する。
- サンプルがどのように適切であり、母集団全体を代表するものであるかを説明する。
- 図 3 は、サンプルサイズを決定するための考慮事項を示しています。

図 3。PCI DSS サンプリングの考慮事項



注：PCI DSS v4.0 では、すべてのテスト手順からサンプリングに関する具体的な言及が削除されました。これらの言及が削除されたのは、一部のテスト手順でサンプリングのみを呼び出すと、そのテスト手順ではサンプリングが必須である（必須ではない）、またはサンプリングが明確に言及された場所でのみ許可されることを示唆する可能性があったためです。評価者は、試験される集団に適切な場合にサンプルを選択すべきであり、上記のように、環境の全体的な範囲と複雑さを考慮した上で、それらの決定を下すべきです。

7 PCI DSS 要件における時間枠の説明

特定の PCI DSS 要件は、定期的にスケジュールされた反復可能なプロセスによって一貫して実行する必要があるアクティビティに対して、特定の時間枠を設定しています。その意図は、アクティビティがその時間枠を超えない範囲で、できるだけ近い間隔で実行されることです。事業体は、指定された頻度よりも高い頻度でアクティビティを実行する裁量権を持ちます（たとえば、PCI DSS 要件で 3 か月ごとに実行するように指定されているアクティビティを毎月実行する）。

表 4 は、PCI DSS 要件で使用されるさまざまな時間帯の頻度の概要を示しています。

表 4。PCI DSS 要件の時間枠

PCI DSS 要件における時間枠	説明と例
毎日	1 年を通じて毎日（営業日に限らず）。
毎週	少なくとも 7 日に 1 回
毎月	30～31 日に 1 回以上、または毎月 n 日に 1 回以上。
3 カ月に 1 回（「四半期」）。	90 日から 92 日に 1 回以上、または 3 カ月目の n 日に 1 回以上。
6 カ月に 1 回	180 日から 184 日に 1 回以上、または 6 カ月目の第 n 日に 1 回以上。
12 カ月に 1 回（「毎年」）	365 日（うるう年の場合は 366 日）ごとに 1 回以上、または毎年同じ日。
定期的に	発生頻度は事業体の裁量に委ねられ、事業体のリスク分析により文書化され、裏付けされます。事業体は、その頻度が、アクティビティが効果的であり、要件の趣旨を満たすために適切であることを実証しなければなりません。
即座	遅滞なく。リアルタイムまたはほぼリアルタイム。

PCI DSS 要件における時間枠	説明と例
迅速	合理的に可能な限り速やかに
大幅な変更	事業体の環境に重大な変化があった場合に、パフォーマンスが規定される要件があります。何をもって大幅な変更とするかは、特定の環境の構成に大きく依存しますが、以下の各アクティビティは、最低限、カード会員データ環境（CDE）のセキュリティに影響を与える可能性があり、関連する PCI DSS 要件のコンテキストにおいて大幅な変更として考慮される必要があります。 • カード会員データ環境（CDE）に追加される新しいハードウェア、ソフトウェア、またはネットワーク機器 • カード会員データ環境（CDE）に追加された新しいハードウェア、ソフトウェア、またはネットワーク機器。カード会員データ環境（CDE）内のハードウェアおよびソフトウェアの交換または主要なアップグレード • アカウントデータのフローまたは保存におけるすべての変更 • カード会員データ環境（CDE）の境界や PCIDSS 評価範囲に対するあらゆる変更 • カード会員データ環境（CDE）の基礎となるサポートインフラへのあらゆる変更（ディレクトリサービス、タイムサーバ、ロギング、監視への変更を含むが、これに限定されない） • カード会員データ環境（CDE） をサポートする、または事業体に代わって PCI DSS 要件を満たすサードパーティベンダ／サービスプロバイダ（または提供されるサービス）に対するすべての変更

その他の PCI DSS 要件で、標準が定期的なアクティビティの最小頻度を定義せず、代わりに要件を「定期的に」満たすことを認めている場合は、事業体がその事業に適した頻度を定義することが期待されます。事業体が定義する頻度は、事業体のセキュリティポリシーおよび PCI DSS 要件 12.3.1 に従って実施されたリスク分析によって裏付けられている必要があります。また、事業体は、定義した頻度のアクティビティが有効であり、要件の意図に合致するために適切であることを実証できる必要があります。

PCI DSS が要求される頻度を規定している場合、および PCI DSS が「定期的な」実行を認めている場合のいずれにおいても、事業体は、少なくとも以下を含む、妥当な時間枠内にアクティビティが実行されることを保証するプロセスを文書化し、実装することが期待されます。

- アクティビティが定義されたスケジュールどおりに実行されない場合はいつでも、事業体に速やかに通知されます。
- 事業体は予定されたアクティビティを欠くことになった事象を判断します。
- 事業体はアクティビティを欠いた後、できるだけ早くアクティビティを実施し、スケジュールに戻すか、新たなスケジュールを設定します。
- 事業体は、上記の要素が発生したことを示す文書を作成します。

事業体が、予定されたアクティビティが行われなかった場合に、それを検知し対処するための上記のプロセスを備えている場合、合理的なアプローチをとることが許容されます。つまり、あるアクティビティを少なくとも 3 カ月に 1 回実施することが要求されている場合、文書化され実施されたプロセス（上記参照）に従っていれば、アクティビティの実施が遅れたとしても、自動的に不適合になるわけではありません。しかし、そのようなプロセスがない場合、や、見落とし、管理ミス、監視の欠如により、アクティビティがスケジュール通りに実行されなかった場合、事業体は要件を満たしていません。このような場合、事業体が 1）予定されたアクティビティが時間通りに行われることを確実にするために、上記のプロセスを文書化（または再確認）し、2）スケジュールを再確立し、3）事業体がスケジュール通りに少なくとも 1 回は予定されたアクティビティを行ったという証跡を提供する場合にのみ、要件は満たされることになります。

注：*初回の PCI DSS 評価（事業体が以前に評価を受けたことがないことを意味する）では、要件にアクティビティを実行する時間枠が定義されている場合、評価者が以下の場合として確認した場合に限り、前年度にその時間枠ごとにアクティビティを実行したことは要求されません。*

- *直近の時間枠（例えば、直近の 3 カ月間または 6 カ月間）において、適用される要件に従ってアクティビティが実施されたこと、および*
- *事業体は、定められた期間内にアクティビティを継続するためのポリシーと手続を文書化しています。*

初回評価以降の年度については、要求される各期間内に少なくとも 1 回、アクティビティが実施されていなければなりません。例えば、3 カ月ごとに実施する必要があるアクティビティは、90-92 日を超えない間隔で、前年度に少なくとも 4 回実施されていなければなりません。

8 PCI DSS の導入と検証のためのアプローチ

セキュリティ目標の達成方法の柔軟性をサポートするために、PCI DSS への実装と検証には 2 つのアプローチがあります。事業体は、自社のセキュリティ実装に最適なアプローチを特定し、そのアプローチを使用してコントロールの検証を行う必要があります。

定義されたアプローチ

PCI DSS を実装および検証するための従来の方法に従い、基準内で定義された要件とテスト手順を使用します。定義されたアプローチでは、事業体は指定された要件を満たすようにセキュリティコントロールを実装し、評価者は定義されたテスト手順に従って、要件が満たされていることを確認します。

定義されたアプローチは、PCI DSS 要件を満たすコントロールが設置されている事業体をサポートします。このアプローチは、セキュリティ目標を達成する方法についてより詳細な指示を求める事業体や、新たに情報セキュリティや PCI DSS を適用する事業体にも適しています。

代替コントロール

定義された手法の一環として、正当かつ文書化された技術上またはビジネス上の制約により、PCI DSS 要件を明示的に満たすことができない事業体は、要件に関連するリスクを十分に軽減する他の*代替コントロール*を実装することができます。年次ベースで、代替コントロールは事業体によって文書化され、評価者によってレビューおよび検証され、準拠に関する報告書の提出に添付される必要があります。

注意：詳細は、付録 B 代替コントロール、付録 C、代替コントロールワークシートをご参照ください。

カスタマイズアプローチ

各 PCI DSS 要件の目的に焦点を当て、事業体が定義された要件に厳密に従っていない方法で、要件に記載されているカスタマイズアプローチの目的を満たすためのコントロールを実装することを許可します。カスタマイズされた実装はそれぞれ異なるため、定義されたテスト手順はありません。評価者は、実装されたコントロールが規定の目的を満たしていることを検証するために、特定の実装に適したテスト手順を導き出す必要があります。

注意：詳細は、付録 D のカスタマイズアプローチ、付録 E のカスタマイズアプローチをサポートするサンプルテンプレートをご参照ください。

カスタマイズアプローチは、セキュリティ対策の導入をサポートし、現在のセキュリティ対策が PCI DSS の目的をどのように満たしているかを事業体がより柔軟に示すことができるようにします。このアプローチは、リスク管理専任部署または事業体全体のリスク管理アプローチなど、セキュリティに対する強固なリスク管理アプローチを実証しているリスク成熟度の高い事業体を対象としています。

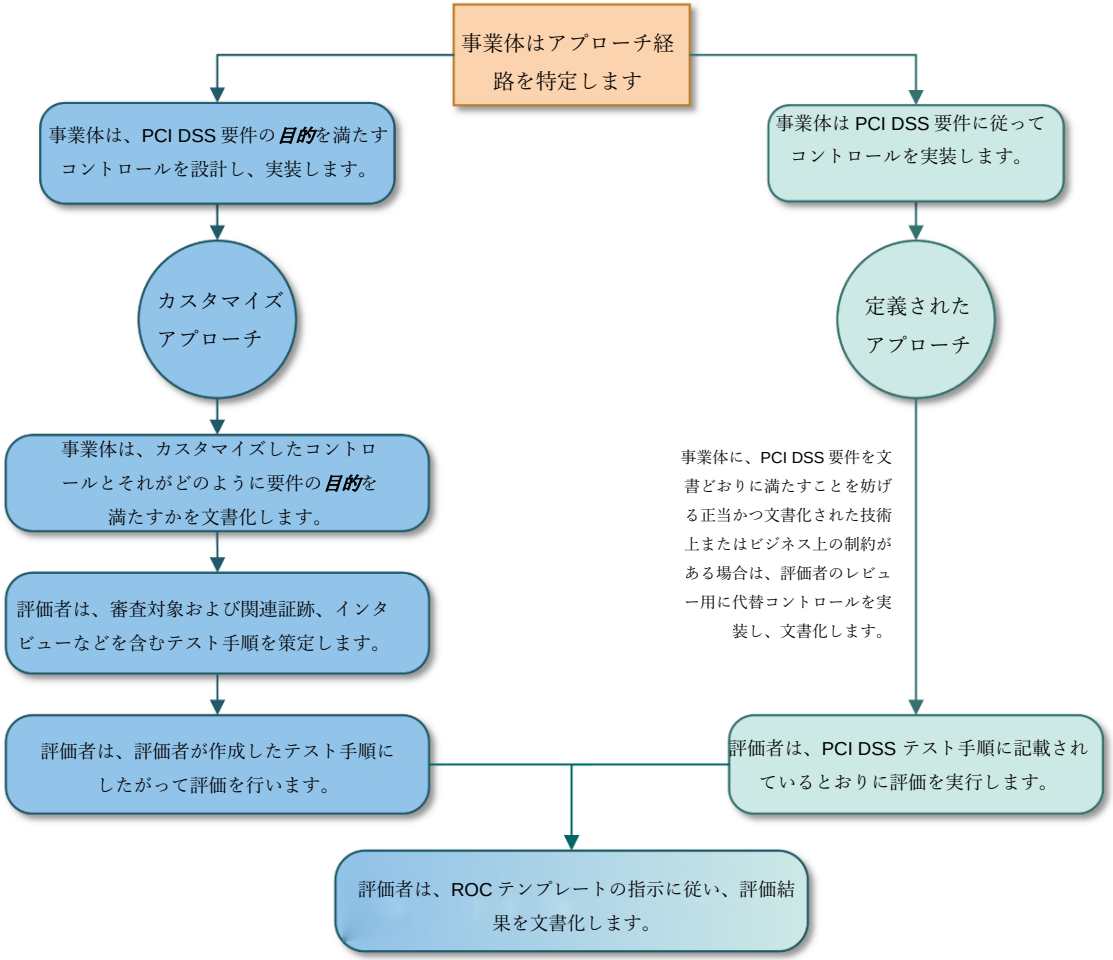
カスタマイズアプローチを使用して実装および検証されたコントロールは、定義されたアプローチの要件によって提供されるセキュリティを満たすか、またはそれを上回ることが期待されます。カスタマイズされた実装を検証するために必要な文書化および労力のレベルも、定義されたアプローチよりも高くなります。

ほとんどの PCI DSS 要件は、定義されたアプローチまたはカスタマイズアプローチのいずれかを使用して満たすことができます。ただし、いくつかの要件にはカスタマイズアプローチの目的が明記されていないため、カスタマイズアプローチはこれらの要件に対するオプションではありません。

事業体は、その環境内で定義されたアプローチとカスタマイズアプローチの両方を使用することができます。つまり、ある事業体は、ある要件を満たすために定義されたアプローチを使用し、他の要件を満たすためにカスタマイズアプローチを使用することができます。これは、事業体が定義されたアプローチを使用して 1 つのシステムコンポーネントまたは環境内の所定の PCI DSS 要件を満たし、カスタマイズアプローチを使用して別のシステムコンポーネントまたは別の環境内の同じ PCI DSS 要件を満たすことができることも意味しています。このように、PCI DSS 評価には、定義されたテスト手順とカスタマイズされたテスト手順の両方が含まれる可能性があります。

図 4 は、PCI DSS v4.0 の 2 つの検証オプションを示しています。

図 4。 PCI DSS 検証アプローチ



9 事業体のセキュリティ体制に関する情報の保護

PCI DSS 準拠環境になり、維持する過程においては、事業体が機密事項とみなし、保護したいと考える多くの成果物が生まれます。これには、次のような項目が含まれます。

- 準拠に関するレポートまたは自己問診票（関連する準拠証明書は機密情報とはみなされず、サードパーティサービスプロバイダ（TPSP）はその AOC を顧客と共有することが期待されます。)
- ネットワーク図とアカウントデータフロー図、セキュリティ設定とルール。
- システム構成基準。
- 暗号と鍵の管理方法とプロトコル。

事業体は、PCI DSS の管理または評価に関連するすべての成果物を確認し、このような機密情報に対する事業体のセキュリティポリシーに従って保護する必要があります。

TPSP は、以下を使用して顧客をサポートすることが要求されています（PCI DSS 要件 12.9）。

- 顧客が TPSP の PCI DSS 準拠状況を監視するために必要な情報（顧客が要件 12.8 に準拠できるようにするため）、および
- TPSP のサービスが顧客の PCI DSS 要件を満たす、または、促進することを意図している場合、また、TPSP のサービスが顧客の カード会員データ環境（CDE） のセキュリティに影響を与える可能性がある場合、TPSP が該当する PCI DSS 要件を満たしていることを示す証跡。

本セクションは、要件 12.9 に従って TPSP が顧客をサポートし、情報を提供する義務に影響を与えたり、否定したりするものではありません。

TPSP に対する期待、および TPSP と顧客との関係の詳細については、サードパーティサービスプロバイダの使用を参照してください。

認定セキュリティ評価機関による秘密かつ機密情報の保護

各 QSA（認定セキュリティ評価者）機関は、QSA の資格要件を順守することを PCI SSC と合意して署名します。その文書の *秘密情報・機密情報の保護*の項には、次のように記載されています。

「QSA 機関は、秘密情報および機密情報の保護に関する文書化されたプロセスを有し、これを順守する必要があります。これには、情報の保管、処理、および／または伝達の間、あらゆる脅威または無許可のアクセスから秘密および機密情報を保護するために、業界で受け入れられている慣行に沿った適切な物理的、電子的、および手続き上の保護手段を含まなければなりません。

QSA は、法的権限により開示が要求されない限り（およびその範囲）、QSA としての任務および義務の遂行過程で入手した情報のプライバシーおよび機密性を維持しなければなりません。」

10 PCI DSS 要件のテスト方法

各要件のテスト手順で特定されるテスト方法は、事業体がその要件を満たしているかどうかを判断するために、評価者が行うべき期待されるアクティビティを記述しています。各テスト方法の意図は、以下のように記述されています。

- 検査：評価者は、証跡となるデータを批判的に評価します。一般的な例としては、文書（電子的または物理的）、スクリーンショット、設定ファイル、監査ログ、データファイルなどがあります。
- 観察：評価者は、評価環境内で行われる行動の監視や評価環境内の対象物の観察を行います。観察対象の例としては、タスクやプロセスを実行する担当者、機能実行や入力に対する応答を行うシステムコンポーネント、環境、物理的なコントロールなどがあります。
- インタビュー：評価者は個々の担当者と会話します。インタビューの目的には、あるアクティビティが行われているかどうかの確認、あるアクティビティがどのように行われているかの説明、担当者が特定の知識や理解を持っているかどうかの確認などが含まれます。

試験方法は、が要件をどのように満たしているかを実証できるようにすることを目的としています。また、事業体および評価者に、実施すべき評価アクティビティに関する共通の理解を提供します。検査または観察される特定の項目およびインタビューされる担当者は、評価される要件および各事業体の特定の実施の両方にとって適切でなければなりません。評価結果を文書化する場合、評価者は、実施した試験アクティビティと各アクティビティの結果を特定します。

11　準拠に関するレポートの指示と内容

準拠報告書（ROC）の説明と内容は、*PCI DSS 準拠報告書（ROC）テンプレート*に記載されています。

PCI DSS 準拠に関する報告書（ROC）テンプレートは、PCI DSS 準拠に関する報告書を作成するためのテンプレートとして使用する必要があります。

PCI DSS への準拠または準拠の検証を必要とする事業体があるかどうかは、準拠プログラムを管理する組織（ペイメントブランドやアクワイアラなど）の裁量によります。事業体は、対象となる組織に連絡して、報告要件や指示を確認する必要があります。

12 PCI DSS 評価プロセス

PCI DSS 評価プロセスには、以下のハイレベルな手順が含まれます。[5]

1. PCI DSS 評価の適用範囲を確認します。
2. PCI DSS の環境評価を実施します。
3. PCI DSS のガイダンスおよび指示に従い、評価に関する該当するレポートを完成させます。
4. サービスプロバイダまたは加盟店に対する、準拠証明書を完成させます。準拠証明書は PCI SSC Web サイトから入手可能です。
5. 該当する PCI SSC 文書および準拠証明書を、ASV スキャンレポートなどその他の要求された文書とともに、要求する組織（ペイメントブランドやアクワイアラ（加盟店の場合）など準拠プログラムを管理する者、またはその他の要求元（サービスプロバイダの場合）に提出します。）
6. 必要に応じて、未対応の要件に対する修正を行い、更新されたレポートを提供します。

注意：*PCI DSS 要件は、コントロールがまだ実装されていない場合、または将来の日付で完了する予定の場合は、実装されているとは見なされません。未実施または未実施の項目が事業体によって対処された後、評価者は、是正が完了し、すべての要件が満たされていることを検証するために再評価を行います。PCI DSS 評価の文書化については、次のリソース（PCI SSC ウェブ サイトで入手可能）を参照してください。*

- *準拠に関するレポート（ROC）の記入方法については、PCI DSS 準拠に関するレポート（ROC） テンプレートを参照してください。*
- *自己問診（SAQ）の記入方法については、PCI DSS SAQ の手順とガイドラインを参照してください。*
- *PCI DSS 準拠の検証レポートの提出方法については、PCI DSS 準拠証明を参照してください。*

[5] PCI DSS 評価プロセス、および各ステップを完了するための役割と責任は、評価の種類や、ペイメントブランドやアクワイアラによって管理されるコンプライアンスプログラムによって異なります。

13　その他の参考資料

表 5 は、PCI DSS 要件または関連するガイダンス内で参照される外部事業体のリストです。これらの外部事業体とその参照先は情報としてのみ提供され、PCI DSS 要件を置き換えたり拡張したりするものではありません。

表 5。 PCI DSS 要件で参照される外部事業体

参照先	名称	出典
ANSI	アメリカ国家規格協会	www.ansi.org
CIS	インターネットセキュリティセンタ	www.cisecurity.org
CSA	クラウドセキュリティアライアンス	www.csa.org
ENISA	欧州連合サイバーセキュリティ機関 （旧欧州ネットワーク情報セキュリティ機関）	www.enisa.europa.eu
FIDO アライアンス	FIDO アライアンス	www.fidoalliance.org
ISO	国際標準化機構	www.iso.org
NCSC	英国国立サイバーセキュリティセンタ	www.ncsc.gov.uk
NIST	米国国立標準技術研究所	www.nist.gov
OWASP	オープンウェブアプリケーションセキュリティプロジェクト	www.owasp.org
SAFEcode	ソフトウェア保証推進フォーラム	www.safecode.org

14 PCI DSS のバージョン

この文書の発行日現在、PCI DSS v3.2.1 は 2024 年 3 月 31 日まで有効であり、それ以降は廃止されます。この日付以降のすべての PCI DSS 検証は、PCI DSS 4.0 またはそれ以降で行わなければなりません。

2022 年 3 月から 2024 年 3 月 31 日の間の評価には、PCI DSS バージョン 3.2.1 または 4.0 のいずれかを使用することができます。

表 6 は、PCI DSS のバージョンとその関連する日付をまとめたものです。[6]

表 6。 PCI DSS のバージョン

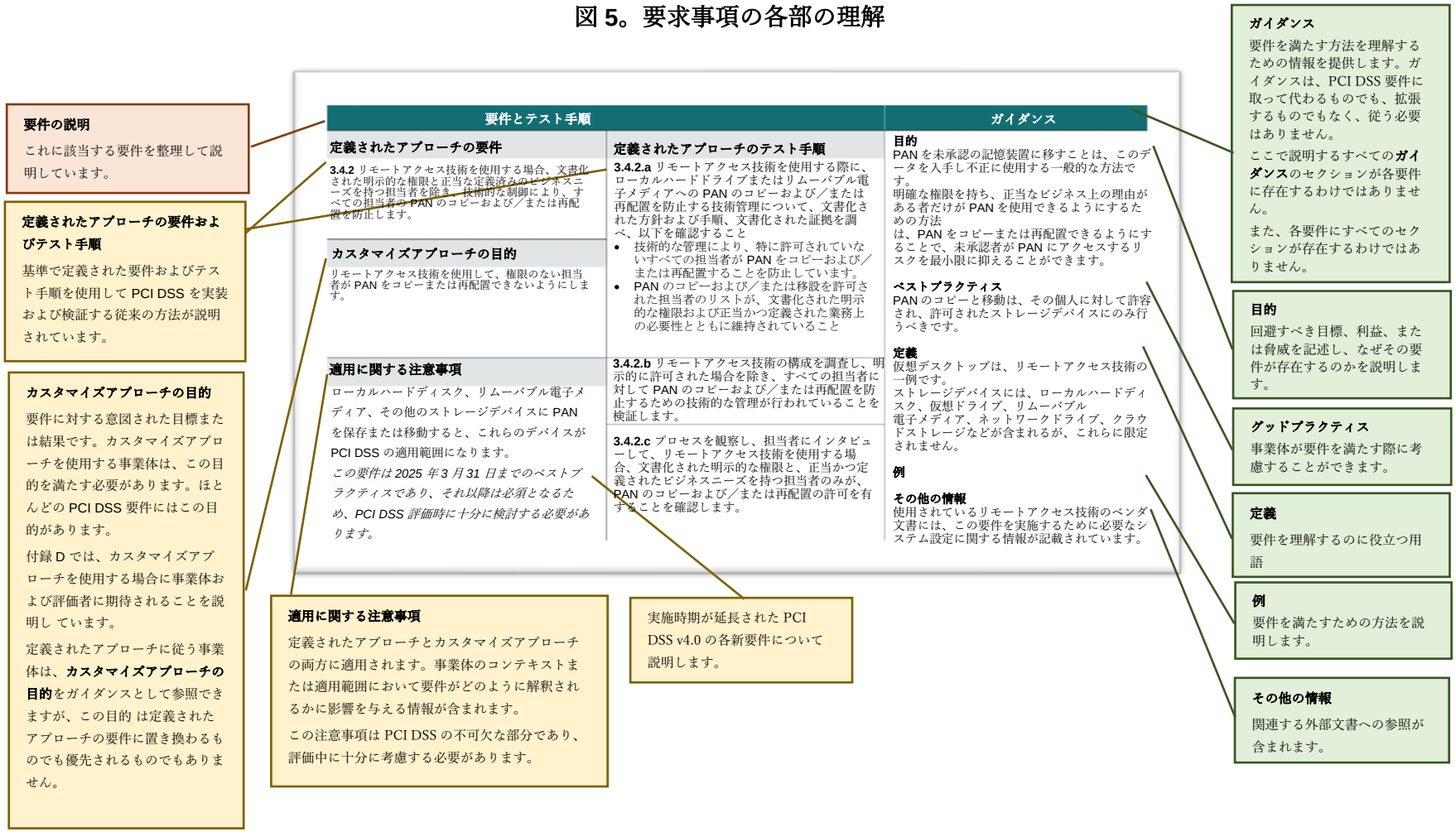
バージョン	公開日	有効期限
PCI DSS v4.0 （本文書）	2022 年 3 月	未定
PCI DSS v3.2.1	2018 年 5 月	2024 年 3 月 31 日

[6] PCI DSS の新バージョンがリリースされた場合、変更される可能性があります。

15 PCI DSS の詳細な要件とテスト手順

図 5 は、PCI DSS の要件の列見出しと内容を説明したものです。

図 5。要求事項の各部の理解



サービスプロバイダのみに対する追加要件

一部の要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用されます。これらは要件内で*「サービスプロバイダのみに対する追加要件」*として特定され、他のすべての適用可能な要件に追加して適用されます。評価対象が加盟店とサービスプロバイダの両方である場合、*「サービスプロバイダのみに対する追加要件」*と記された要件が、事業体のサービスプロバイダ部分に適用されます。*「サービスプロバイダのみに対する追加要件」*と記載されている要件は、すべての事業体が考慮すべきベストプラクティスとして推奨されます。

*さまざまな種類の事業体に対する追加の **PCI DSS** 要件を記載した付録*

PCI DSS 付録 A には、12 の主要要件に加え、さまざまな種類の事業体に対する追加の PCI DSS 要件が記載されています。付録 A 内のセクションは以下の通り:

- 付録 A1:マルチテナント型サービスプロバイダに対する追加の PCI DSS 要件。
- 付録 A2:カード提示の POS POI 端末接続に SSL／初期の TLS を使用する事業者に対する追加の PCI DSS 要件。
- 付録 A3:指定事業者の補足的検証（DESV。）

安全なネットワークとシステムの構築と維持

要件 1：ネットワークセキュリティコントロールの導入と維持

セクション	
1.1	ネットワークセキュリティコントロールを導入・維持するためのプロセスや仕組みが定義され、理解されている。
1.2	ネットワークセキュリティコントロール（NSC）が設定され、維持されている。
1.3	カード会員データ環境への、およびカード会員データ環境からのネットワークアクセスが制限され ている。
1.4	信頼できるネットワークと信頼できないネットワーク間の接続が制御されている。
1.5	信頼されないネットワークとカード会員データ環境（CDE）の両方に接続できるコンピューティングデバイスによるカード会員データ環境（CDE）へのリスクは軽減される。

概要

ファイアウォールやその他のネットワークセキュリティ技術などのネットワークセキュリティコントロール（NSC）は、ネットワークポリシーの実施ポイントであり、通常、事前に定義された*ポリシー*または*ルール*に基づいて、2 つ以上の論理的または物理的なネットワークセグメント（またはサブネット）間のネットワークトラフィックを制御する。

NSC は、セグメントに入る（ingress）、出る（egress）すべてのネットワークトラフィックを検査し、定義されたポリシーに基づいて、ネットワークトラフィックの通過を許可するか、拒否するかを決定する。通常、NSC は異なるセキュリティニーズや信頼レベルの環境間に設置されるが、信頼レベルの境界とは関係なく個々のデバイスへのトラフィックを制御する環境もある。ポリシーの適用は一般的に OSI モデルの第 3 層で行われるが、より高い層に存在するデータもポリシー決定のために頻繁に使用される。

従来、この機能は物理ファイアウォールによって提供されてきたが、現在では仮想デバイス、クラウドアクセスコントロール、仮想化／コンテナシステム、その他のソフトウェア定義ネットワーキング技術によって提供される場合がある。

NSC は、事業者自身のネットワーク内のトラフィック（例えば、機密性の高いエリアと低いエリア間）を制御し、事業者のリソースが信頼されないネットワークにさらされないように保護するために使用される。カード会員データ環境（CDE）は、企業のネットワーク内でより機密性の高い領域の一例である。信頼されていないネットワークとの間の一見些細な経路が、保護されていない機密システムへの侵入経路になることがよくある。NSC は、あらゆるコンピュータ・ネットワークに重要な保護メカニズムを提供する。

信頼できないネットワークの一般的な例としては、インターネット、企業間通信チャネルなどの専用接続、無線ネットワーク、キャリアネットワーク（携帯電話など）、サードパーティーネットワーク、その他企業の管理能力の及ばないソースがある。さらに、信頼されないネットワークには、PCI DSS の適用範囲外とみなされる企業ネットワークも含まれる。これらの企業ネットワークは評価されていないことから、セキュリティコントロールの存在が検証されていないため、信頼されないものとして扱わなければならないからである。企業はインフラの観点から内部ネットワークを信頼できると考えるかもしれないが、ネットワークが PCI DSS の適用範囲外である場合、そのネットワークは PCI DSS に対して信頼できないネットワークと見なさなければならない。

PCI DSS 用語の定義については、*付録 G* を参照してください。

要件とテスト手順		ガイダンス
1.1 ネットワークセキュリティコントロールを導入・維持するためのプロセスや仕組みが定義され、理解されている。		
定義されたアプローチの要件 **1.1.1** 要件 1 で特定されたすべてのセキュリティポリシーと運用手順が、 • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に周知されている。 **カスタマイズアプローチの目的** 要件 1 内の活動を満たすために期待されること、コントロール、および監視活動が、影響を受ける担当者によって定義、理解、および順守されている。すべての支援活動が繰り返し可能であり、一貫して適用され、経営者の意図に適合している。	**定義されたアプローチのテスト手順** **1.1.1** 要件 1 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューする。	**目的** 要件 1.1.1 は、要件 1 を通して指定された様々なポリシーと手順を効果的に管理し、維持することに関する要件です。要件 1 で指定された特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及していることを確認することも同様に重要です。 **グッドプラクティス** プロセス、技術、業務目的の変化に対応するため、ポリシーと手順を必要に応じて更新することが重要です。そのため、定期的な更新だけでなく、変更があった場合はできるだけ早く更新することを検討してください。 **定義** セキュリティポリシーは、企業のセキュリティの目的および原則を定義するものです。運用手順は、活動の実行方法を記述し、一貫した方法で、ポリシーの目的に従って望ましい結果を達成するために従うコントロール、方法、プロセスを定義します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要な活動が行われない可能性があります。 **グッドプラクティス** 役割と責任は、方針と手順の中で文書化されるか、または別の文書で管理されるかもしれません。 事業体は、担当者が各自に与えられた役割と責任を受け入れ理解するよう、役割と責任を伝える必要があります。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担表（RACI 表とも呼ばれる）があります。
1.1.2 要件 1 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**1.1.2.a** 文書を調査し、要件 1 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	1.1.2.b 要件 1 の活動の実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 1 のすべての活動を実行するための日常的な責任が割り当てられている。担当者は、これらの要件の成功、継続的な運用に責任を負っている。		

要件とテスト手順		ガイダンス
1.2 ネットワークセキュリティコントロール（NSC）が設定され、維持されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
1.2.1 NSC ルールセットの構成基準が • 定義されている。 • 実装されている。 • 維持されている。	**1.2.1.a** NSC ルールセットの構成基準を調べ、その基準がこの要件で指定されたすべての要素に準拠していることを確認する。	これらの構成基準を実施することにより、NSC はそのセキュリティ機能を適切に発揮できるように構成・管理されることになります（しばしばルールセットと呼ばれる）。
カスタマイズアプローチの目的	**1.2.1.b** NSC ルールセットの構成設定を調べ、ルールセットが構成基準に従って実装されていることを確認する。	**グッドプラクティス** これらの標準は、多くの場合、許容されるプロトコルの要件、使用が許可されるポート、および許容される特定の構成要件を定義しています。また、構成基準には、事業体がネットワーク内で許容できない、または許可できないと考えるものを概説する場合もあります。
NSC の設定と動作の方法が定義され、一貫して適用されていること。		**定義** NSC は、ネットワークアーキテクチャの重要な構成要素です。最も一般的に、NSC は カード会員データ環境（CDE） の境界で使用され、カード会員データ環境（CDE） から出入りするネットワークトラフィックを制御します。 構成基準は、その NSC の構成に関する事業体の最小要件の概要を示します。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		例 本構成基準の対象となる NSC の例としては、ファイアウォール、アクセス制御リストを設定したルータ、 クラウド仮想ネットワークなどが挙げられますが、これらに限定されるものではありません。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**グッドプラクティス**
1.2.2 ネットワーク接続および NSC の構成に対する全ての変更は、要件 6.5.1 で定義された変更管理プロセスに従って承認および管理する。	**1.2.2.a** 文書化された手順を調査し、ネットワーク接続および NSC の構成の変更が要件 6.5.1 に従った正式な変更管理プロセスに含まれることを確認する。	変更は、変更の影響を理解するために適切な権限と知識を持つ個人によって承認されるべきです。検証は、変更がネットワークのセキュリティに悪影響を及ぼさないこと、および変更が期待通りに実行されることを合理的に保証するものでなければなりません。 変更によって生じたセキュリティ上の問題への対処を回避するため、すべての変更は実施前に承認され、変更実施後に検証される必要があります。承認・検証後は、ネットワーク文書と実際の構成との間に矛盾が生じないように、変更を含むようにネットワーク文書を更新する必要があります。
	1.2.2.b ネットワーク構成設定を調査し、ネットワーク接続に加えられた変更を特定する。担当者にインタビューを行い、変更管理記録を調査し、特定されたネットワーク接続の変更が要件 6.5.1 に従って承認、管理されていることを確認する。	
カスタマイズアプローチの目的	**1.2.2.c** ネットワーク構成設定を調査し、NSC の構成に加えられた変更を特定する。担当者にインタビューを行い、変更管理記録を調査し、特定された NSC の設定変更が要件 6.5.1 に従って承認および管理されていることを確認する。	
ネットワーク接続や NSC の変更により、誤設定、安全でないサービスの実装、または未承認のネットワークへの接続が発生しないようにする。		
適用に関する注意事項		
ネットワーク接続の変更には、接続の追加、削除、または修正が含まれる。 NSC の設定の変更には、コンポーネント自体に関連するものと、そのセキュリティ機能の実行方法に影響を与えるものが含まれる。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
1.2.3 カード会員データ環境（CDE）と他のネットワーク（無線ネットワークを含む）間のすべての接続を示す正確なネットワーク図が維持されている。	**1.2.3.a** この要件で指定されたすべての要素に従って正確なネットワーク図が存在することを確認するために、図を調べ、ネットワーク構成を観察する。 **1.2.3.b** 文書を調査し、担当者にインタビューして、ネットワーク図が正確であること、環境に変更があった場合に更新されることを確認する。	正確で最新のネットワーク図を維持することで、ネットワークの接続や機器の見落としを防ぎ、知らず知らずのうちに安全が確保されず、侵害されやすい状態になることを防ぎます。 適切に維持管理されたネットワーク図は、カード会員データ環境（CDE） に接続するシステムおよび カード会員データ環境（CDE） から接続されるシステムを識別することで、事業体が PCI DSS の適用範囲を検証するのに役立ちます。 **グッドプラクティス** カード会員データ環境（CDE）のシステムコンポーネントに対してセキュリティ、管理、またはメンテナンスサービスを提供するシステムを含め、カード会員データ環境（CDE）とのすべての接続を識別する必要があります。事業体は、ネットワーク図に以下を含めることを検討する必要があります。 • 小売店、データセンタ、企業拠点、クラウドプロバイダなどを含むすべての拠点 *(次ページに続く)*
カスタマイズアプローチの目的		
カード会員データ環境（CDE）、全ての信頼できるネットワーク、および全ての信頼されないネットワーク間の境界が構築・維持され、利用可能であること		
適用に関する注意事項		
ネットワークの接続と機器を特定した最新のネットワーク図、またはその他の技術的もしくはトポロジを表すソリューションを使用して、この要件を満たすことができる。		

要件とテスト手順		ガイダンス
		• すべてのネットワークセグメントの明確なラベル付け • 各コントロールを一意に識別できるもの（例えば、コントロールの名前、メーカー、モデル、およびバージョン）を含む、セグメンテーションを提供するすべてのセキュリティコントロール • NSC、ウェブアプリファイアウォール、アンチマルウェアソリューション、変更管理ソリューション、IDS／IPS、ログ集約システム、決済端末、ペイメントアプリケーション、HSM など、適用範囲内のすべてのシステムコンポーネント • 適用範囲外の領域がある場合は、図中に網掛けなどの方法で明確に表示すること • 最終更新日、更新者名および承認者名 • ダイアグラムを説明するための凡例または要点 図がネットワークの正確な説明を提供し続けることを確実にするために、権限のある担当者が図を更新する必要があります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 最新のデータフロー図は、アカウントデータがネットワーク上や個々のシステム、機器間でどのように流れているかを示すことで、事業体が環境の範囲を理解し、追跡するのに役立ちます。 最新のデータフロー図を維持することで、アカウントデータが見落とされたり、知らないうちにセキュリティが確保されないまま放置されることを防ぐことができます。 **グッドプラクティス** データフロー図には、オープンな公共ネットワークへの接続、アプリケーション処理のフロー、ストレージ、システムとネットワーク間の送信、ファイルのバックアップなど、アカウントデータがネットワークに送受信されるすべての接続点を含める必要があります。 データフロー図は、ネットワーク図に追加するものであり、ネットワーク図と整合させ、補強するものである必要があります。ベストプラクティスとして、事業体は、データフロー図に以下を含めることを検討できます。 • アカウントデータのすべての処理フロー（オーソリゼーション、キャプチャ、決済、チャージバック、および払い戻しを含む） *(次ページに続く)*
1.2.4 以下を満たす正確なデータフロー図が整備されている • システムおよびネットワーク上のすべてのアカウントデータの流れが示されている。 • 環境変化に伴い、必要に応じて更新されている。	**1.2.4.a** データフロー図を調査し、担当者にインタビューして、この要件で指定されたすべての要素に従って、すべてのアカウントデータのフローが示されていることを確認する。	
カスタマイズアプローチの目的 システムコンポーネント間およびネットワークセグメント間のアカウントデータの全ての伝送が表現されたものが維持され、利用可能である。	**1.2.4.b** ドキュメントを調査し、担当者にインタビューして、データフロー図が正確であり、環境に変更があった場合は更新されていることを確認する。	
適用に関する注意事項 システムおよびネットワークにわたるアカウントデータの流れを特定するデータフロー図、またはその他の技術的もしくはトポロジを表すソリューションを使用して、この要件を満たすことができる。		

要件とテスト手順		ガイダンス
		• カード提示型、カード非提示型、電子商取引など、異なるすべての受け入れチャネル • ハードコピー／紙媒体を含む、あらゆるタイプのデータ受信または送信 • アカウントデータが環境に入る時点から、最終的な処分までの流れ • アカウントデータが伝送および処理される場所、保存される場所、および保存が短期間か長期的か • 受け取ったすべてのアカウントデータの発生源（例えば、顧客、第三者など）、およびアカウントデータを共有するすべての事業体 • 最終更新日、更新者名および承認者名

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 未使用または安全でないサービス（例：telnet や FTP）、プロトコル、ポートが原因で脆弱性が発生することがよくあります。これは、カード会員データ環境（CDE）に不必要なアクセスポイントを開いてしまうことにつながるからです。さらに、有効であっても使用されていないサービス、プロトコル、およびポートは見落とされがちで、安全が確保されずパッチも適用されないまま放置されることがあります。業務に必要なサービス、プロトコル、ポートを特定することで、その他のサービス、プロトコル、ポートのすべてを確実に無効化または削除することができます。 **グッドプラクティス** 許可された各サービス、プロトコル、ポートに関連するセキュリティリスクを理解する必要があります。承認は、構成を管理する担当者から独立した担当者が行うべきです。承認者は、承認を判断するために適切な知識と説明責任を有するべきです。 **目的** 侵害は、安全でないネットワーク設定を利用します。 *(次ページに続く)*
1.2.5 許可されたすべてのサービス、プロトコル、ポートが特定され、承認され、業務上の必要性が定義されている。	**1.2.5.a** ドキュメントを調査し、業務上の正当性とそれぞれの承認を含む、許可されたすべてのサービス、プロトコル、およびポートのリストが存在することを確認する。	
	1.2.5.b NSC の構成設定を調査し、承認されたサービス、プロトコル、およびポートのみが使用されていることを確認する。	
カスタマイズアプローチの目的 未承認のネットワークトラフィック（サービス、プロトコル、特定ポート宛てのパケット）がネットワークに出入りできないようにする。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
1.2.6 使用されていて安全でないと見なされるすべてのサービス、プロトコル、およびポートについて、リスクを軽減するようなセキュリティ機能が定義され、実装されている。	**1.2.6.a** 使用されているすべての安全でないサービス、プロトコル、ポートを特定する文書を調査し、それぞれについて、リスクを軽減するためのセキュリティ機能が定義されていることを確認する。	
カスタマイズアプローチの目的 安全でないサービス、プロトコル、ポートの使用に関連する特定のリスクを理解し、評価し、適切に軽減することができる。	**1.2.6.b** NSC の構成設定を調査し、特定された安全でないサービス、プロトコル、ポートそれぞれについて、定義されたセキュリティ機能が実装されていることを確認する。	

要件とテスト手順		ガイダンス
		グッドプラクティス 安全でないサービス、プロトコル、ポートが業務上必要な場合、これらのサービス、プロトコル、ポートがもたらすリスクを事業体が明確に理解し、受け入れ、サービス、プロトコル、ポートの使用を正当化し、これらのサービス、プロトコル、ポートの使用リスクを軽減するセキュリティ機能を事業体で定義し実装する必要があります。 **その他の情報** 安全でないとみなされるサービス、プロトコル、またはポートに関するガイダンスについては、業界標準やガイダンス（例えば、NIST、ENISA、OWASP によるガイド）を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** このような見直しは、不正な者によって利用される可能性のある、不要な、古い、あるいは誤ったルールや設定を一掃する機会を事業体に与えます。さらに、すべてのルールと設定が、文書化された業務上の正当な理由に合致する、認可されたサービス、プロトコル、およびポートのみを許可することを保証します。 **グッドプラクティス** このレビューは、手動、自動、またはシステムベースの方法を用いて実施することができ、トラフィックルールを管理する設定、つまりネットワークへの出入りを許可するものが承認された設定と一致していることを、確認することを目的としています。 このレビューでは、許可されたすべてのアクセスに正当な業務上の理由があることを確認する必要があります。ルールや設定に関する不一致や不明な点は、解決のためにエスカレーションされるべきです。 この要件では、このレビューを少なくとも 6 カ月に 1 回実施するよう規定していますが、ネットワーク設定の変更量が多い事業体は、設定が引き続き業務上の必要性を満たしていることを確実にするために、より頻繁にレビューを実施することを検討してもよいでしょう。
1.2.7 NSC の設定は、少なくとも 6 カ月に 1 回は見直しを行い、適切かつ効果的であることを確認する。	**1.2.7.a** 少なくとも 6 カ月に 1 回は NSC の設定をレビューするための手順が定義されていることを確認するために文書を調査する。	
	1.2.7.b NSC の設定の見直しに関する文書を調査し、担当者にインタビューして、少なくとも 6 カ月に 1 回レビューが行われていることを確認する。	
カスタマイズアプローチの目的 信頼されたネットワークへのアクセスを許可または制限する NSC 設定を定期的に検証し、現在の業務上の正当性を伴う認可された接続のみが許可されることを確認する。	**1.2.7.c** NSC の設定を調査し、業務上の正当な理由によりサポートされなくなったと特定された設定が削除または更新されていることを確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
1.2.8 NSC の構成ファイルが • 不正なアクセスから保護されている。 • アクティブなネットワーク構成と整合性が保たれている。	**1.2.8** NSC の構成ファイルを調査し、この要件で指定されたすべての要素に従っていることを確認する。	不正な設定がネットワークに適用されることを防ぐため、ネットワーク制御の設定を保存したファイルは常に最新の状態に保ち、不正な変更から保護する必要があります。 設定情報を最新かつ安全に保つことで、設定を実行するたびに、NSC の正しい設定が適用されます。 **例** ルータの安全な設定が不揮発性メモリに保存されている場合、そのルータが再起動またはリブートされたときに、これらの制御で、その安全な設定が復元されることを確実にする必要があります。
カスタマイズアプローチの目的		
信頼できない設定オブジェクト（ファイルを含む）を使用して、NSC を定義または修正することはできない。		
適用に関する注意事項		
NSC の設定または同期に使用されるあらゆるファイルまたは設定は、"構成ファイル "とみなされる。これには、バックアップ、アーカイブ、遠隔保存されている、ファイル、自動化されたシステムベースのコントロール、スクリプト、設定、IaC（Infrastructure as Code）、または他のパラメータが含まれる。		

要件とテスト手順		ガイダンス
1.3 カード会員データ環境へのネットワークアクセスおよびカード会員データ環境からのネットワークアクセス が制限されている。		
定義されたアプローチの要件 **1.3.1** カード会員データ環境（CDE）への着信トラフィックは、以下のように制限される。 • 必要なトラフィックのみにする。 • それ以外のトラフィックは明確に拒否される。 **カスタマイズアプローチの目的** 未承認のトラフィックがカード会員データ環境（CDE）に侵入できない。	**定義されたアプローチのテスト手順** **1.3.1.a** NSC の構成基準を調査し、カード会員データ環境（CDE）への着信トラフィックの制限が定義され、この要件で指定されたすべての要素に従っていることを確認する。 **1.3.1.b** NSC の設定を調べ、カード会員データ環境（CDE）への着信トラフィックがこの要件で指定されたすべての要素に従って制限されていることを確認する。	**目的** この要件は、悪意のある個人が不正な IP アドレスを介して事業体のネットワークにアクセスしたり、不正な方法でサービス、プロトコル、ポートを使用することを防止することを目的としています。 **グッドプラクティス** カード会員データ環境（CDE）に流入するすべてのトラフィックは、それがどこから発生したかにかかわらず、確立された認可されたルールに従っていることを確認するために評価されるべきです。例えば、送信元／送信先アドレスやポートの制限、コンテンツのブロックなどにより、トラフィックが認可された通信のみに制限されていることを確認するために、接続を検査する必要があります。 **例** 例えば、明示的な「deny all」や allow 文の後に暗黙的な deny を使用するなどして、特に必要のないすべての着信および発信トラフィックを拒否するルールを実装することで、意図しない潜在的に有害なトラフィックの許可を防止することに役立ちます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** この要件は、事業体のネットワーク内の悪意のある個人および侵害されたシステムコンポーネントが、信頼されていない外部ホストと通信することを防止することを目的としています。 **グッドプラクティス** カード会員データ環境（CDE）から発信されるすべてのトラフィックは、送信先にかかわらず、確立され、認可されたルールに従っていることを確実にするために評価されるべきです。例えば、送信元／送信先のアドレスやポートを制限したり、コンテンツをブロックすることで、許可された通信のみにトラフィックを制限するために、接続を検査する必要があります。 **例** 例えば、明示的な「deny all」や allow 文の後に暗黙的な deny を使用するなどして、特に必要のないすべての着信およびアウトバウンドトラフィックを拒否するルールを実装することで、意図しない潜在的に有害なトラフィックの許可を防止することに役立ちます。 *(次ページに続く)*
1.3.2 カード会員データ環境（CDE）からの発信トラフィックは、以下のように制限される。 • 必要なトラフィックのみにする。 • それ以外のトラフィックは明確に拒否される。	**1.3.2.a** NSC の構成基準を調査し、この要件で指定されたすべての要素に従ってカード会員データ環境（CDE）からの発信トラフィックの制限を定義していることを確認する。	
カスタマイズアプローチの目的 未承認のトラフィックはカード会員データ環境（CDE）から出ることができない。	**1.3.2.b** NSC の設定を調査し、この要件で指定されたすべての要素に従ってカード会員データ環境（CDE）からの発信トラフィックが制限されていることを確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
1.3.3 NSC は、無線ネットワークがカード会員データ環境（CDE）であるかどうかに関わらず、すべての無線ネットワークとカード会員データ環境（CDE）の間に以下のように実装する。 • 無線ネットワークからカード会員データ環境（CDE）へのすべての無線トラフィックは、デフォルトで拒否される。 • 許可された業務目的の無線トラフィックのみがカード会員データ環境（CDE）に許可される。	**1.3.3** 構成設定とネットワーク図を調べ、この要件で指定されたすべての要素に従って、すべての無線ネットワークとカード会員データ環境（CDE）の間に NSC が実装されていることを確認する。	ネットワーク内の無線技術の既知（または未知）の実装と悪用は、悪意のある個人がネットワークとアカウントデータにアクセスするための共通の経路です。事業体が知らないうちに無線機器や無線ネットワークが設置されていた場合、悪意のある個人が簡単に、そして「見えないように」ネットワークに侵入することができます。NSC が無線ネットワークからカード会員データ環境（CDE）へのアクセスを制限しない場合、無線ネットワークに不正にアクセスした悪意のある個人が簡単にカード会員データ環境（CDE）に接続し、アカウント情報を危険にさらす可能性があります。
カスタマイズアプローチの目的		
カード会員データ環境（CDE）内のあらゆる無線ネットワークと有線環境の間で、不正なトラフィックがネットワーク境界を通過できない。		

要件とテスト手順		ガイダンス
1.4 信頼できるネットワークと信頼できないネットワーク間のネットワーク接続が制御されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
1.4.1 NSC を、信頼できるネットワークと信頼できないネットワークの間で実装する。	**1.4.1.a** 構成基準やネットワーク図を調べ、信頼できるネットワークと信頼できないネットワークの間で NSC が定義されていることを確認する。	信頼できるネットワークに発着信する全ての接続に NSC を実装することにより、事業体はアクセスを監視、制御することができ、悪意のある個人が保護されていない接続を介して内部ネットワークにアクセスする機会を最小化することができます。
	1.4.1.b ネットワーク構成を調べ、文書化された構成基準およびネットワーク図に従って、信頼できるネットワークと信頼できないネットワークの間に NSC が設置されていることを確認する。	**例**
カスタマイズアプローチの目的		DMZ は、信頼できないネットワーク（信頼できないネットワークの例については「要件 1 の概要」を参照）と、ウェブサーバなど事業体が一般に公開する必要があるサービスとの間の接続を管理するネットワークの一部であり、事業体が実装することもあります。事業体の DMZ がアカウントデータを処理または送信する場合（例：電子商取引ウェブサイト）、それもカード会員データ環境（CDE）とみなされることに注意してください。
信頼できるネットワークと信頼できないネットワークの間で、不正なトラフィックがネットワークの境界を通過することができない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
1.4.2 信頼できないネットワークから信頼できるネットワークへの着信トラフィックは、以下に制限される。 • 一般に公開されたサービス、プロトコル、ポートを提供することが許可されているシステムコンポーネントとの通信。 • 信頼できるネットワーク内のシステムコンポーネントによって開始された通信に対するステートフルな応答。 • その他のトラフィックはすべて拒否。	**1.4.2** NSC のベンダ文書および構成を調査し、信頼できないネットワークから信頼できるネットワークへの着信トラフィックが、この要件で指定されたすべての要素に従って制限されていることを確認する。	**目的** システムコンポーネントへのパブリックアクセスが特別に許可されていることを確実にすることで、システムコンポーネントが信頼できないネットワークに不必要にさらされるリスクを低減することができます。 **グッドプラクティス** 電子メール、ウェブ、DNS サーバなど、一般に公開されたサービスを提供するシステムコンポーネントは、信頼できないネットワークから発信される脅威に対して最も脆弱です。 このような一般に公開されるシステム（例、DMZ など）は、NSC によってより機密性の高い内部システムから分離された専用の信頼できるネットワーク内に配置することが理想的です。これらは外部からアクセス可能なシステムが侵害された場合に、その他の部分を保護することに役立ちます。この機能は、悪意のある攻撃者がインターネットから事業体の内部ネットワークにアクセスしたり、サービス、プロトコル、ポートを不正に使用したりすることを防ぐことを目的としています。 この機能が NSC の組込機能として提供される場合、事業体は、この機能が無効化されたり、バイパスされたりしないことを確実にする必要があります。 *(次ページに続く)*
カスタマイズアプローチの目的		
信頼できるネットワーク内のシステムコンポーネントに対して許可された、または応答するトラフィックのみが、信頼できないネットワークから信頼できるネットワークに入ることができる。		
適用に関する注意事項		
この要件の意図は、プロトコルの仕様よりも、信頼できるネットワークと信頼できないネットワーク間の通信セッションを扱うことである。 この要件は、ステータスが NSC によって維持される場合、UDP または他のコネクションレス型ネットワークプロトコルの使用を制限するものではない。		

要件とテスト手順		ガイダンス
		定義 ネットワークへの各接続のステータスを維持することは、以前の接続に対する明確な応答でも、（NSC は各接続の状態を保持しているため）有効で承認された応答であるのか、あるいは NSC を欺いて接続を許可しようとする悪意のあるトラフィックであるのかを 、NSC が判別できることを意味します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 信頼できるネットワークに流入するパケットをフィルタリングすることは、特に、パケットが事業体内部のネットワークから来たように見える「なりすまし」がないことを確認するのに役立ちます。例えば、スプーフィング対策により、インターネットから発信された内部アドレスが DMZ に侵入するのを防ぐことができます。 **グッドプラクティス** 通常、製品にはスプーフィング対策がデフォルトで設定されていますが、設定できない場合もあります。詳細については、ベンダ文書を参照してください。 **例** 通常、パケットにはそれを送信したコンピュータの IP アドレスが含まれており、ネットワーク内の他のコンピュータは、そのパケットがどこから送信されたかを知ることができます。 悪意のある攻撃者は、しばしば送信元の IP アドレスをなりすまし（または模倣）して、ターゲットのシステムを騙して、パケットが信頼できる送信元からのものであると信じ込ませようとすることがあります。
1.4.3 偽造された送信元 IP アドレスが信頼できるネットワークに侵入するのを検知しブロックするためにスプーフィング対策を実施する。	**1.4.3** NSC のベンダ文書および設定を調査し、偽造された送信元 IP アドレスが信頼できるネットワークに侵入することを検出しブロックするために、スプーフィング対策が実施されていることを確認する。	
カスタマイズアプローチの目的		
偽造された IP 送信元アドレスを持つパケットは、信頼できるネットワークに入ることができない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
1.4.4 カード会員データを保存するシステムコンポーネントは、信頼できないネットワークから直接アクセス できないようにする。	**1.4.4.a** データフロー図とネットワーク図を調べ、カード会員データを保存するシステムコンポーネントが信頼できないネットワークから直接アクセスできないことが文書化されていることを確認する。	カード会員データが DMZ 内のシステムやクラウドデータベースサービスに保存されているなど、信頼できないネットワークから直接アクセスできる場合、侵入を妨げる防御層が少ないため、外部の攻撃者がアクセスしやすくなります。NSC を使用して、カード会員データを保存するシステムコンポーネント（データベースやファイルなど）が信頼できるネットワークからのみ直接アクセスできるようにすることで、不正なネットワークトラフィックがシステムコンポーネントに到達するのを防ぐことができます。
カスタマイズアプローチの目的	**1.4.4.b** NSC の構成を調べ、カード会員データを保存するシステムコンポーネントが信頼できないネットワークから直接アクセスできないような制御が実施されていることを確認する。	
保存されたカード会員データに、信頼できないネットワークからアクセスできないようにする。		
適用に関する注意事項		
この要件は、揮発性メモリへのアカウントデータの保存には適用されないが、メモリが永続的ストレージとして扱われる場合（例えば、RAM ディスク）には適用される。アカウントデータは、関連する業務プロセスをサポートするために必要な期間（例えば、関連するペイメントカード取引が完了するまで）でのみ、揮発性メモリに保存することができる。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 内部 IP アドレス、プライベート IP アドレス、ローカル IP アドレスの開示を制限することは、悪意のある攻撃者がこれらの IP アドレスを知り、その情報を使ってネットワークにアクセスすることを防ぐために有効です。 **グッドプラクティス** この要件の意図を満たすために使用される方法は、使用される特定のネットワーク技術によって異なる場合があります。例えば、この要件を満たすために使用される制御は、IPv4 ネットワークと IPv6 ネットワークでは異なる場合があります。 **例** IP アドレスをわかりにくくする方法としては、以下のものが考えられますが、これらに限定されるものではありません。 • IPv4 ネットワークアドレス変換（NAT） • プロキシサーバ／NSC の背後にシステムコンポーネントを配置する。 • 登録されたアドレスを使用する内部ネットワークのルータ広告（IPv6 RA）の削除またはフィルタリング *(次ページに続く)*
1.4.5 内部 IP アドレスやルーティング情報の開示は、許可された関係者のみに限定される。	**1.4.5.a** NSC の構成を調査し、内部の IP アドレスとルーティング情報の開示が許可された者のみに限定されていることを確認する。	
	1.4.5.b 担当者にインタビューを行い、文書を調査し、内部の IP アドレスおよびルーティング情報の開示が許可された関係者のみに限定されるような管理が実施されていることを確認する。	
カスタマイズアプローチの目的		
内部ネットワーク情報が不正な開示から保護されている。		

要件とテスト手順		ガイダンス
		• インターネットへの送信セッションを開始する際に、RFC 1918（IPv4）を内部で使用するか、IPv6 プライバシー拡張（RFC 4941）を使用する。

要件とテスト手順		ガイダンス
1.5 信頼できないネットワークとカード会員データ環境（CDE）の両方に接続できるコンピューティングデバイスによるカード会員データ環境（CDE）へのリスクが軽減されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
1.5.1 信頼できないネットワーク（インターネットを含む）とカード会員データ環境（CDE）の両方に接続する、事業体や従業員が所有するデバイスを含むあらゆるコンピューティングデバイスに対し、以下のようにセキュリティ管理を実施する。 • 事業体のネットワークに脅威が侵入するのを防ぐために、特定の構成設定を定義する。 • セキュリティ管理がアクティブに実行中である。 • セキュリティ管理は、特に文書化され、管理者から期間を限ってケースバイケースで承認されない限り、コンピューティングデバイスのユーザによって変更できないようになっている。	**1.5.1.a** ポリシーと構成基準を調査し、担当者にインタビューして、信頼できないネットワークとカード会員データ環境（CDE）の両方に接続するコンピューティングデバイスのセキュリティ管理が、この要件で指定されているすべての要素に従って実装されていることを確認する。	デスクトップ、ノートパソコン、タブレット、スマートフォン、その他従業員が使用するモバイルコンピューティングデバイスなど、事業体の環境の外からインターネットへの接続が許可されているコンピューティングデバイスは、インターネットベースの脅威に対してより脆弱になりがちです。 ホストベースのセキュリティ管理（パーソナルファイアウォールソフトウェアやエンドポイントプロテクションソリューションなど）、ネットワークベースのセキュリティ管理（ファイアウォール、ネットワークベースのヒューリスティック検査、マルウェアシミュレーションなど）、またはハードウェアなどのセキュリティ管理を使用することにより、デバイスがネットワークに再接続されたときに、デバイスを使用して事業体のシステムやデータにアクセスするようなインターネットベースの攻撃から、デバイスを保護することができます。 *(次ページに続く)*
カスタマイズアプローチの目的	**1.5.1.b** 信頼できないネットワークとカード会員データ環境（CDE）の両方に接続するコンピューティングデバイスの構成設定を調べ、この要件で指定されているすべての要素に従って設定が実装されていることを確認する。	
信頼できない環境に接続し、カード会員データ環境（CDE）にも接続するデバイスには、事業体のカード会員データ環境（CDE）に脅威をもたらす可能性がある。		

要件とテスト手順		ガイダンス
適用に関する注意事項 これらのセキュリティ管理は、技術的に正当な必要性があり、管理者がケースバイケースで承認した場合にのみ、一時的に無効化することができる。特定の目的のためにこれらのセキュリティ管理を無効にする必要がある場合、正式に承認されなければならない。また、これらのセキュリティ管理が無効になっている間、追加のセキュリティ対策が必要になる場合もある。 この要件は、従業員所有のコンピューティングデバイスと事業体所有のコンピューティングデバイスに適用される。事業体のポリシーで管理できないシステムは、弱点をもたらし、悪意のある個人に脆弱性を突いた攻撃の機会を与えることになる。		**グッドプラクティス** 具体的な構成設定は、事業体が決定し、そのネットワークセキュリティポリシーおよび手順と一致させる必要があります。 信頼できないネットワークと カード会員データ環境（CDE） の両方に接続する事業体所有または従業員所有のデバイスのセキュリティコントロールを一時的に無効にする正当な必要性がある場合（例えば、特定の保守活動または技術的問題の調査をサポートするため）には、それらの対応を行う理由を理解し、適切な管理担当者によって承認がされます。管理者自身のデバイスを含め、これらのセキュリティ制御の無効化または変更は、権限を与えられた担当者によって行われます。 管理者には、自身のコンピュータのセキュリティ制御を無効にできる権限を有していると認識していても、そのような制御が無効にされた場合に警告する仕組みがあり、プロセスが順守されたことを確認するためのフォローアップが行われる必要があります。 **例** 従業員所有または事業体所有のモバイルデバイスの VPN のスプリットトンネルを禁止し、そのようなデバイスは VPN で起動することを義務付ける等があります。

要件 2：　すべてのシステムコンポーネントにセキュアな設定を適用する

セクション
2.1 すべてのシステム構成要素にセキュアな設定を適用するためのプロセスと仕組みが定義され、理解されている。
2.2 システムコンポーネントは安全に設定され、管理されている。
2.3 無線環境が安全に設定され、管理されている。

概要

悪意のある個人は、企業の外部と内部の両方で、しばしばデフォルトパスワードや他のベンダのデフォルト設定を使用してシステムを侵害する。これらのパスワードや設定はよく知られており、公開情報を介して容易に特定することができる。

システムの構成要素に安全な設定を施すことで、攻撃者がシステムを侵害するために利用できる手段を減らすことができる。デフォルトパスワードの変更、不要なソフトウェア、機能、アカウントの削除、不要なサービスの無効化または削除はすべて、潜在的な攻撃対象領域を減らすのに有効である。

PCI DSS 用語の定義については、付録 G を参照。

要件とテスト手順		ガイダンス
2.1 すべてのシステムコンポーネントにセキュアな設定を適用するためのプロセスと仕組みが定義され、理解されている。		
定義されたアプローチの要件 **2.1.1** 要件 2 で特定されたすべてのセキュリティポリシーと運用手順が • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に周知されている。	**定義されたアプローチのテスト手順** **2.1.1** 要件 2 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調べ、担当者にインタビューを行う。	**目的** 要件 2.1.1 は、要件 2 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 2 で呼び出された特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及していることを確実にすることも同様に重要であす。 **グッドプラクティス** プロセス、技術、業務目的の変化に対応するため、ポリシーと手順を必要に応じて更新することが重要です。このため、定期的な更新だけでなく、変更があった場合はできるだけ早く更新することを検討してください。 **定義** セキュリティポリシーは、事業体のセキュリティの目的および原則を定義するものです。 運用手順は、活動の実行方法を説明するもので、ポリシーの目的に沿って一貫した方法で望ましい結果を得るために従う管理、方法、プロセスを定義するものです。
カスタマイズアプローチの目的 要件 2 内の活動を満たすための期待、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべての支援活動が繰り返し可能であり、一貫して適用され、マネジメントの意図に適合している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要な活動が行われない可能性があります。 **グッドプラクティス** 役割と責任は、方針と手順の中で文書化することもできるし、別の文書で管理することもできます。 役割と責任を伝える一環として、事業体は、担当者に割り当てられた役割と責任を受け入れ、理解したことを認めさせることを検討することができます。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を記載した責任分担表（RACI 表とも呼ばれる）があります。
2.1.2 要件 2 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**2.1.2.a** 文書を調査し、要件 2 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	2.1.2.b 要件 2 の活動実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 2 のすべての活動を実施するための日常的な責任が割り当てられている。担当者は、これらの要件の成功させ、継続的に運用する責任を負う。		

要件とテスト手順		ガイダンス
2.2 システムの構成要素が安全に設定され、管理されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
2.2.1 構成基準は、以下の目的で開発、実施、維持する。 • すべてのシステムコンポーネントをカバーする。 • すべての既知のセキュリティ脆弱性に対処する。 • 業界で認められているシステム堅牢化の標準またはベンダの堅牢化の推奨と整合している。 • 要件 6.3.1 に定義されているように、新しい脆弱性の問題が特定されたときに更新される。 • システムコンポーネントが本番環境に接続される前、または直後に、新しいシステムが構成され、適切であることが確認された場合に適用される。	**2.2.1.a** システム構成基準を調査し、この要件で指定されたすべての要素を含むプロセスを定義していることを確認する。 **2.2.1.b** 要件 6.3.1 で定義されているように、新たな脆弱性の問題が特定されるとシステム構成基準が 更新されることを確認するために、方針と手順を調査し、担当者にインタビューを行う。 **2.2.1.c** 構成設定を調査し、担当者にインタビューして、新しいシステムを構成する際にシステム構成基準が適用され、システムコンポーネントが本番環境に接続される前または直後にシステム構成基準が適用されている状態にあることが確認されること。	事業体が使用する、または事業体の環境内で使用される多くのオペレーティングシステム、データベース、ネットワークデバイス、ソフトウェア、アプリケーション、コンテナイメージ、その他のデバイスには既知の弱点が存在します。また、セキュリティ上の脆弱性を修正するために、これらのシステムコンポーネントを設定する方法も知られています。セキュリティの脆弱性を修正することで、攻撃者が利用できる機会を減らすことができます。 基準を策定することにより、事業体は、システムコンポーネントが一貫して安全に構成されることを確実にし、完全な堅牢化が困難なデバイスの保護に対処することができます。
カスタマイズアプローチの目的		**グッドプラクティス**
すべてのシステムコンポーネントは、業界で認められた堅牢化標準またはベンダの推奨に従って、安全かつ一貫性をもって構成されている。		業界の最新のガイダンスに従うことは、安全な構成を維持するのに役立ちます。 システムに適用される具体的なコントロール方法は様々であり、システムの種類と機能に応じて適切である必要があります。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		多くのセキュリティ機関がシステム堅牢化のガイドラインと推奨事項を制定しており、一般的で既知の弱点を修正する方法をアドバイスしています。 **その他の情報** 構成基準に関するガイダンスの情報源は以下のとおりですが、これらに限定されるものではありません。インターネットセキュリティセンター（CIS）、国際標準化機構（ISO）、米国国立標準技術研究所（NIST）、クラウドセキュリティアライアンス(CSA)、製品ベンダなど。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
2.2.2 ベンダのデフォルトアカウントは、以下のように管理する。 • ベンダのデフォルトアカウントを使用する場合、デフォルトパスワードは要件 8.3.6 に従って変更する。 • ベンダのデフォルトアカウントを使用しない場合、そのアカウントは削除または無効化する。	**2.2.2.a** システム構成基準を調査し、この要件で指定されたすべての要素に従ってベンダのデフォルトアカウントの管理が含まれていることを確認する。 **2.2.2.b** ベンダのドキュメントを調査し、システム管理者がベンダのデフォルトアカウントを使用してログオンしているところを観察して、この要件で指定されているすべての要素に従ってアカウントが実装されていることを確認する。 **2.2.2.c** 設定ファイルを調査し、担当者にインタビューして、使用しないすべてのベンダのデフォルトアカウントが削除または無効化されていることを確認する。	悪意のある個人は、多くの場合ベンダのデフォルトアカウント名とパスワードを使用して、それがインストールされているオペレーティングシステム、アプリケーション、およびシステムを侵害します。これらのデフォルト設定は公開されることが多く、よく知られていますが、設定を変更することで攻撃に対するシステムの脆弱性を軽減することができます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 システムコンポーネントは、デフォルトのパスワードを使用してアクセスできない。 **適用に関する注意事項** これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーションとシステムアカウント、POS 端末、ペイメントアプリケーション、SNMP（Simple Network Management Protocol）のデフォルトなどで使用される、すべてのベンダのデフォルトアカウントとパスワードに適用される。 この要件は、システムコンポーネントが事業者の環境内にインストールされていない場合にも適用される。例えば、カード会員データ環境（CDE）の一部であり、クラウド契約サービスを通じてアクセスされるソフトウェアやアプリケーション。		**グッドプラクティス** すべてのベンダのデフォルトアカウントを特定し、その目的と使用方法を理解する必要があります。クラウドサービスのデプロイや保守に使用するアカウントも含め、アプリケーションやシステムのアカウントについては、デフォルトのパスワードを使用せず、権限のない個人が使用できないような管理することが重要です。 デフォルトアカウントの使用を意図していない場合、デフォルトパスワードを PCI DSS 要件 8.3.6 を満たす一意のパスワードに変更し、デフォルトアカウントへのアクセスをすべて削除してからそのアカウントを無効にすると、悪意のある個人がそのアカウントを再び有効にしてデフォルトパスワードでアクセスすることを防止できます。 新しいシステムのインストールと構成には、分離されたステージングネットワークを使用することが推奨され、また、それによりデフォルトの認証情報が本番環境に導入されないことを確実にすることができます。 **例** デフォルトとして考慮すべきは、ユーザ ID、パスワード、その他、ベンダが自社製品で一般的に使用している認証情報などです。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
2.2.3 異なるセキュリティレベルを必要とする主機能は、以下のように管理される。 • 1 つのシステムコンポーネントに存在する主機能は 1 つだけである。 **または** • 同じシステムコンポーネント上に存在するセキュリティレベルの異なる主機能は、互いに分離されている。 **または** • 同じシステムコンポーネント上のセキュリティレベルの異なる主機能は、すべてが最もセキュリティの必要性の高い機能が要求するレベルまでセキュリティが確保されている。	**2.2.3.a** システム構成基準を調査し、この要件に規定されているように、異なるセキュリティレベルを必要とする主機能を管理することが含まれていることを確認する。 **2.2.3.b** システム構成を調査し、異なるセキュリティレベルを必要とする主機能が、この要件で指定された方法のいずれかによって管理されていることを確認する。 **2.2.3.c** 仮想化技術を使用する場合、システム構成を検証し、異なるセキュリティレベルを必要とするシステム機能が、以下のいずれかの方法で管理されていることを確認する。 • セキュリティニーズの異なる機能が、同じシステムコンポーネント上に共存しない。 • 同じシステムコンポーネント上に存在する異なるセキュリティニーズを持つ機能が、互いに分離されている。 • 同じシステムコンポーネント上にあるセキュリティニーズの異なる機能はすべて、最も高いセキュリティニーズを持つ機能が要求するレベルにまでセキュリティが確保されている。	**目的** 主要な機能のためのサービス、プロトコル、デーモンの組み合わせを含むシステムは、その機能が効果的に動作するように適切なセキュリティプロファイルを持つことになります。例えば、インターネットに直接接続する必要があるシステムは、DNS サーバ、ウェブ サーバ、e コマースサーバのように特定のプロファイルを持つことになるでしょう。逆に、他のシステムコンポーネントは、事業体がインターネットに公開したくない機能を実行する、サービス、プロトコル、デーモンの異なるセットからなる主要な機能を動作させるでしょう。この要件は、異なる機能が他のサービスのセキュリティプロファイルに影響を与えて、他のサービスがより高いまたはより低いセキュリティレベルで動作することにならないようにすることを目的としています。 **グッドプラクティス** 理想的には、各機能は異なるシステムコンポーネントに配置されるべきです。これには、各システムコンポーネントに主機能を 1 つだけ実装することで実現できます。別の方法として、例えば、インターネットに直接接続する必要があるウェブサーバを、アプリケーションサーバやデータベースサーバと分離するなど、セキュリティレベルの異なる主機能を同じシステムコンポーネント上に分離することもできます。 *(次ページに続く)*
カスタマイズアプローチの目的		
セキュリティニーズの低い主機能が、同じシステムコンポーネント上のセキュリティニーズの高い主機能のセキュリティに影響を与えることがないようにする。		

要件とテスト手順		ガイダンス
		システムコンポーネント内に異なるセキュリティレベルを必要とする主機能がある場合の、第三の選択肢は、セキュリティニーズの高い主機能のセキュリティレベルが、セキュリティレベルの低い主機能の存在によって低下しないように、追加の管理策を導入することです。さらに、セキュリティレベルの低い機能は、他のシステム機能のリソースにアクセスしたり影響を与えたりできないように分離および／または保護し、同じサーバ上の他の機能にセキュリティ上の弱点をもたらさないようにする必要があります。 異なるセキュリティレベルの機能は、物理的または論理的な管理によって分離することができます。例えば、データベースシステムは、仮想化技術などの制御を使用して機能を分離し、別のサブシステムに格納しない限り、ウェブ サービスも提供すべきではありません。また、仮想インスタンスを使用したり、システム機能ごとに専用のメモリアクセスを提供したりするのも一例です。 仮想化技術を使用する場合、各仮想コンポーネントについてセキュリティレベルを特定し、管理する必要があります。仮想化環境における考慮事項の例としては、以下のようなものがあります。 • アプリケーション、コンテナ、または仮想サーバインスタンスごとの機能。 • 仮想マシン（VM）やコンテナの保存方法とセキュリティの確保の方法。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
2.2.4 必要なサービス、プロトコル、デーモン、機能のみを有効化し、不要な機能はすべて削除または無効化する。	**2.2.4.a** システム構成基準を調査し、必要なシステムサービス、プロトコル、デーモンが特定され、文書化されていることを確認する。	不要なサービスや機能は、悪意のある個人がシステムにアクセスするための新たな機会を提供する可能性があります。不要なサービス、プロトコル、デーモン、機能をすべて削除または無効化することで、事業体は必要な機能の保護に集中でき、未知の機能や不要な機能が悪用されるリスクを低減することができます。
カスタマイズアプローチの目的	**2.2.4.b** システムのコンポーネント構成を調べ、以下を確認する。 • 不要な機能がすべて削除または無効化されている。 • 構成基準に記載されている必要な機能のみが有効化されている。	**グッドプラクティス** デフォルトで有効になっている可能性のあるプロトコルの中には、悪意のある人物がネットワークを侵害するためによく使用するものが多くあります。例えば、使用していないサービス、機能、プロトコルをすべて無効化または削除すること（例えば、FTP やウェブ サーバの削除や無効化）で、潜在的な攻撃対象領域を最小化することができます。
システムコンポーネントに存在する不要な機能を悪用し、システムコンポーネントを危険にさらすことができないようにする。		**例** 不要な機能には、スクリプト、ドライバ、機能、サブシステム、ファイルシステム、インタフェース（USB、Bluetooth）、不要なウェブ サーバなどが含まれますが、これらに限定されません。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
2.2.5 安全でないサービス、プロトコル、デーモンが存在する場合、 • ビジネス上の正当性が文書化されている。 • 安全でないサービス、プロトコル、またはデーモンを使用するリスクを低減するための追加のセキュリティ機能が文書化され、実装されている。	**2.2.5.a** 安全でないサービス、プロトコル、またはデーモンが存在する場合、システム構成基準を調査し、担当者にインタビューして、それらがこの要件で指定されているすべての要素に従って管理および実装されていることを確認する。	すべての安全でないサービス、プロトコル、デーモンが適切なセキュリティ機能で充分に保護されていることを確認することで、悪意のある個人がネットワーク内の共通の侵害ポイントを悪用することがより困難になります。
カスタマイズアプローチの目的	**2.2.5.b** 安全でないサービス、プロトコル、デーモンが存在する場合、構成設定を調査し、安全でないサービス、デーモン、プロトコルを使用するリスクを低減するために追加のセキュリティ機能が実装されていることを確認する。	**グッドプラクティス**
安全でないサービス、プロトコル、またはデーモンを悪用することによって、システムコンポーネントを危険にさらすことができないようにする。		新しいシステムコンポーネントを導入する前にセキュリティ機能を有効にすることで、安全でない設定が環境に導入されるのを防ぐことができます。ベンダのソリューションによっては、安全でないプロセスを保護するための追加のセキュリティ機能が提供されている場合があります。
		その他の情報
		安全でないと考えられるサービス、プロトコル、デーモンに関するガイダンスについては、業界標準やガイダンス（例えば、NIST、ENISA、OWASP が発行するものなど）を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
2.2.6 システムのセキュリティパラメータが誤使用を防止するように設定されている。	**2.2.6.a** システム構成基準を調査し、誤使用を防止するためのシステムセキュリティパラメータの構成が含まれていることを確認する。	システムコンポーネントが提供するセキュリティパラメータを正しく設定することで、システムコンポーネントの機能を活用し、悪意のある攻撃に打ち勝つことができます。
	2.2.6.b システム管理者および／またはセキュリティ管理者にインタビューし、システムコンポーネントの一般的なセキュリティパラメータ設定について知識を有していることを確認する。	**グッドプラクティス** システム構成基準および関連プロセスは、使用するシステムの種類ごとに、セキュリティ上の影響があることが分かっているセキュリティ設定やパラメータを具体的に扱う必要があります。
カスタマイズアプローチの目的	**2.2.6.c** システムコンポーネントを調査し、共通セキュリティパラメータがシステム構成基準に従って適切に設定されていることを確認する。	システムを安全に構成するためには、システムの構成および／または管理を担当する担当者は、システムに適用される特定のセキュリティパラメータおよび設定に精通している必要があります。また、クラウドポータルへのアクセスに使用されるパラメータの安全な設定についても考慮する必要があります。
セキュリティパラメータが正しく設定されていないために、システムコンポーネントが危険にさらされることはない。		**その他の情報** システムの種類ごとに適用可能なセキュリティパラメータについては、要件 2.2.1 で述べたベンダの文書や業界の参考文献を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
2.2.7 コンソール以外のすべての管理者アクセスは、強力な暗号を使用して暗号化する。	**2.2.7.a** システム構成基準を調査し、コンソール以外のすべての管理者アクセスを強力な暗号を使用して暗号化することが含まれていることを確認する。	**目的** 非コンソール管理者アクセス（リモート含む）で暗号化通信を使用しない場合、管理者の認証要素（IDやパスワードなど）が盗聴者に知られる可能性があります。悪意のある者は、この情報を利用してネットワークにアクセスし、管理者になり、データを盗むことができます。 **グッドプラクティス** どんなセキュリティプロトコルを使用するにしても、安全でない接続の使用を防ぐため、安全なバージョンと設定のみを使用するように設定する必要があります。例えば、信頼できる証明書のみを使用し、強力な暗号化のみをサポートし、より弱い安全でないプロトコルや方法へのフォールバックに対応しない、などです。 **例** HTTP や telnet などの平文プロトコルは、トラフィックやログオンの詳細を暗号化しないので、盗聴者がこれらの情報を簡単に傍受することができます。帯域外（OOB）、Lights-Out Management（LOM）、インテリジェント・プラットフォーム管理インタフェイス（IPMI）、リモート機能付きのキーボード・ビデオ・マウス（KVM）スイッチなどを含め、これらに限らず、システムへ別のアクセスができるようになる技術によって、コンソール以外からのアクセスが容易になる場合があります。これら
	2.2.7.b 管理者がシステムコンポーネントにログオンするのを観察し、システム構成を調査して、コンソール以外の管理者アクセスがこの要件に従って管理されていることを確認する。	
	2.2.7.c システムコンポーネントと認証サービスの設定を調査し、コンソール以外の管理者アクセスで安全でないリモートログインサービスが利用できないことを確認する。	
カスタマイズアプローチの目的 平文の管理認証因子は、いかなるネットワーク伝送からも読み取られたり、傍受されたりすることはない。	**2.2.7.d** ベンダの文書を調査し、担当者にインタビューを行い、使用中の技術に応じた強力な暗号が業界のベストプラクティスおよび／またはベンダの推奨に従って実装されていることを確認する。	
適用に関する注意事項 ブラウザベースのインタフェースやアプリケーションプログラミングインタフェース（API）を介した管理者アクセスも含まれる。		

要件とテスト手順		ガイダンス
		や、その他のコンソール以外のアクセス技術や方法は、強力な暗号技術で保護しなければなりません。 **その他の情報** *NIST SP 800-52* や *SP 800-57* などの業界標準やベストプラクティスを参照してください。

要件とテスト手順		ガイダンス
2.3 無線環境が安全に設定され、管理されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
2.3.1 カード会員データ環境（CDE）に接続する、またはアカウントデータを送信する無線環境では、インストール時にすべての無線ベンダのデフォルトを変更するか、または、安全であることを確認する。これには以下が含まれるが、これらに限定されない。 • デフォルトのワイヤレス暗号化キー • パスワードまたはワイヤレスアクセスポイント • SNMP のデフォルト • その他のセキュリティ関連のワイヤレスベンダのデフォルト	**2.3.1.a** ポリシーと手順を調査し、担当者にインタビューして、無線ベンダのデフォルトについて、インストール時に変更するか、この要件のすべての要素に従って安全であることを確認するためのプロセスが定義されていることを確認する。	無線ネットワークは、十分なセキュリティ設定（デフォルト設定の変更も含む）が行われていないと、無線スニッファーがトラフィックを盗聴し、データやパスワードを簡単に取得し、ネットワークに簡単に侵入して攻撃することができます。
	2.3.1.b ベンダのドキュメントを調べ、システム管理者が無線機器にログインしているところを観察して以下を確認する。 • SNMP のデフォルトが使用されていないこと。 • アクセスポイントのデフォルトのパスワード／パスフレーズが使用されていないこと。	**グッドプラクティス** 無線 LAN のパスワードは、オフラインの総当たり攻撃（ブルートフォース攻撃）に耐えられるように構築する必要があります。
カスタマイズアプローチの目的 ベンダのデフォルトパスワードやデフォルト設定を使用して、ワイヤレスネットワークにアクセスすることができない。	**2.3.1.c** ベンダの文書および無線構成設定を調査し、該当する場合は、その他のセキュリティ関連の無線ベンダのデフォルトが変更されていることを確認する。	
(次ページに続く)		

要件とテスト手順		ガイダンス
適用に関する注意事項 これには、デフォルトの無線暗号化キー、無線アクセスポイントのパスワード、SNMP のデフォルト、およびその他のセキュリティ関連の無線ベンダのデフォルトが含まれますが、これに限定されない。		
定義されたアプローチの要件 **2.3.2** カード会員データ環境（CDE）に接続し、アカウントデータを送信する無線環境では、無線暗号鍵は以下のように変更する。 • 鍵の知識を持つ担当者が、会社またはその知識が必要であった役割を離れた都度 • 鍵の漏洩が疑われる場合、または判明した都度 **カスタマイズアプローチの目的** 無線暗号鍵の知識があると、無線ネットワークへの不正なアクセスを防ぐことができる。	**定義されたアプローチのテスト手順** **2.3.2** 担当者にインタビューを行い、鍵管理文書を調査し、無線暗号鍵がこの要件で指定されているすべての要素に従って変更されていることを確認する。	**目的** 無線暗号鍵を知っている人が事業体を離れたり、鍵を知る必要のない役割に異動したりするたびに、無線暗号鍵を変更することで、鍵の知識を、知る必要のある人だけに限定しておくことができます。 また、暗号鍵の漏えいが疑われる場合や、漏えいが判明した場合は常に、無線暗号鍵を変更することで、無線ネットワークの耐障害性を向上させることができます。 **グッドプラクティス** この目標は、定期的な鍵の交換、定義された「採用・異動・退職」（JML）プロセスを通しての鍵の交換、追加の技術的な管理策の実装、固定の事前共有鍵（PSK）の不使用などを含めて、複数の方法で達成することができます。 さらに、漏洩したことが判明している、または漏洩の疑いがある鍵は、要件 12.10.1 での事業体のインシデント対応計画に従って管理されるべきです。

アカウントデータの保護

要件 3：　保存されたアカウントデータの保護

セクション	
3.1	保存されているアカウントデータを保護するためのプロセスとメカニズムが定義され、理解されている。
3.2	アカウントデータの保存を最小限にとどめる。
3.3	機密認証データ（SAD）は、オーソリゼーション後に保存されない。
3.4	PAN 全体の表示へのアクセス、および PAN のコピー機能が制限されている。
3.5	プライマリアカウント番号（PAN）は、保存場所に関わらず、保護されている。
3.6	保存されているアカウントデータを保護するために使用される暗号化鍵が保護されている。
3.7	保存されているアカウントデータを保護するために暗号が使用されている場合、鍵のライフサイクルの すべての側面を網羅する鍵管理プロセスおよび手順が定義され、実施されている。

概要

暗号化、トランケーション、マスキング、ハッシュなどの保護方法は、アカウントデータ保護の重要な構成要素です。侵入者が他のセキュリティコントロールを回避して、暗号化されたアカウントデータにアクセスできても、そのデータは正しい暗号化鍵がなければ読み取れず、その侵入者は使用することはできません。保存されたデータを保護するその他の効果的な方法も、リスク軽減の機会として考慮する必要があります。例えば、リスクを最小限に抑える方法として、必要な場合以外はアカウントデータを保存しない、完全な PAN が不要な場合はカード会員データを切り捨てる、電子メールやインスタントメッセージなどのエンドユーザメッセージングテクノロジを使って保護されていない PAN を送信しない、などがあります。

アカウントデータが非永続的メモリ（RAM、揮発性メモリなど）に存在する場合、アカウントデータの 暗号化は必要ありません。しかし、メモリが非永続的な状態を維持するように適切な管理が行われなければなりません。データは、業務の目的（例えば、関連するトランザクション）が完了した時点で、揮発性メモリから削除される必要があります。データの保存が永続的になった場合、保存データの暗号化を含め、適用可能なすべての PCI DSS 要件が適用されます。

要件 3 は、個別の要件で特に言及されていない限り、保存されたアカウントデータの保護に適用されます。

「強力な暗号化技術」およびその他の PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
3.1 保存されているアカウントデータを保護するためのプロセスとメカニズムが定義され、理解されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 要件 3.1.1 は、要件 3 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 3 で指定された特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、周知されていることを確認することも同様に重要です。 **グッドプラクティス** プロセス、技術、ビジネス目的の変化に対応するため、ポリシーと手順を必要に応じて更新することが重要です。そのため、定期的な更新だけでなく、変更があった場合はできるだけ早く更新することを検討してください。 **定義** セキュリティポリシーは、事業体のセキュリティの目的および原則を定義するものです。運用手順は、活動の実行方法を記述し、一貫した方法で、ポリシーの目的に従って望ましい結果を達成するためのコントロール、方法、プロセスを定義します。
3.1.1 要件 3 で特定されたすべてのセキュリティポリシーと運用手順が • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に周知されている。	**3.1.1** 要件 3 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューする。	
カスタマイズアプローチの目的		
要件 3 内の活動を充足するための期待、コントロール、および監視活動が定義され、影響を受ける担当者によって順守されている。すべての支援活動が再現可能であり、一貫して適用され、経営者の意図に適合している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要な活動が行われない可能性があります。 **グッドプラクティス** 役割と責任は、方針と手順の中で文書化されるか、または別の文書で管理されるかもしれません。 役割と責任を伝える一環として、事業体は、担当者に与えられた役割と責任を受け入れ、理解したことを認めさせることを検討することができます。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担表（RACI マトリクスとも呼ばれる）があります。
3.1.2 要件 3 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**3.1.2.a** 文書を調査し、要件 3 の活動を行う役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	3.1.2.b 要件 3 の活動を実施する責任を有する担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 3 のすべての活動を実施するための日常的な責任が割り当てられている。担当者は、これらの要件の効果的、継続的な運用に説明責任を負う。		

要件とテスト手順		ガイダンス
3.2 アカウントデータの保存を最小限にとどめる。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
3.2.1 アカウントデータの保存は、少なくとも以下を含むデータ保持・廃棄ポリシー、手順、プロセスの実施により、最小限にとどめる。 • アカウントデータが保存されているすべての場所を対象とする。 • オーソリゼーションが完了するまでに保存されているすべての機密認証データ（SAD）を対象とする。*この箇条は、発効日まではベストプラクティスである。詳細については、以下の「適用に関する注意事項」を参照。* • データの保存量および保存期間を、法律、規制、および／または事業上の要件に必要なものに限定する。 • 保存されたアカウントデータの保存期間を定義し、文書化された業務上の正当な理由を含む、特定の保存要件。 • 保持ポリシーに基づき、不要になったアカウントデータを安全に削除する、または復元不可能にするためのプロセス。 • 定義された保存期間を超えて保存されたアカウントデータが安全に削除されたこと、または復元不可能にされたことを少なくとも 3 カ月に一度、検証するためのプロセス。	**3.2.1.a** データ保持と廃棄のポリシー、手順、プロセスを調査し、担当者にインタビューして、この要件で指定されているすべての要素を含むようにプロセスが定義されていることを確認する。 **3.2.1.b** アカウントデータが保存されているシステムコンポーネント上のファイルおよびシステムレコードを調査し、データの保存量および保存期間がデータ保持ポリシーに定義された要件を超えないことを確認する。 **3.2.1.c** アカウントデータを復元不可能にするためのメカニズムを観察し、データが復元できないことを確認する。	**目的** 正式なデータ保持ポリシーは、どのデータをどれくらいの期間保持する必要があるか、またそのデータがどこに存在するかを特定し、不要になったらすぐに安全に破棄または削除できるようにするものです。オーソリゼーション後に保存される可能性のあるアカウントデータは、プライマリアカウント番号または PAN（読み取り不可にされたもの）、有効期限、カード会員名、サービスコードのみです。 オーソリゼーションプロセス完了前の 機密認証データ（SAD）の保存もデータ保持・廃棄ポリシーに含まれ、この機密 データの保存は最小限に抑えられ、定められた期間のみ保持されます。 **グッドプラクティス** アカウントデータの保存場所を特定する際には、データにアクセスできるすべてのプロセスと担当者を考慮します。なぜなら、データは当初定義された場所とは異なる場所に移動され保存されている可能性があるからです。見落とされがちな保存場所としては、バックアップやアーカイブシステム、取り外し可能なデータ保存デバイス、紙ベースのメディア、オーディオ録音などがあります。 *(次ページに続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 アカウントデータは必要な場合のみ、必要最小限の期間保持され、不要になった場合は安全に削除または復元不可能な状態にされる。		適切な保存要件を定義するためには、事業体はまず自社のビジネスニーズを理解し、業界や保存するデータの種類に適用される法的または規制上の義務を理解する必要があります。また、定義された保存期間に基づいて、自動的かつ安全にデータを削除する自動化プロセスを導入することで、ビジネス、法律、規制上の必要以上にアカウントデータを保持しないようにすることができます。 保存期間を超えたデータの消去方法には、データを完全に除去するための安全な削除、またはデータを復元不可能にして、再構築できないようにする方法があります。保存期間を超えた保存データを特定し、安全に消去することで、不要になったデータの保存を防ぐことができます。このプロセスは、自動化、手動化、またはその両方の組み合わせが可能です。 ほとんどの OS の削除機能は、削除したデータを復元できるため「安全な削除」ではありません。そのため、代わりに専用の安全な削除機能またはアプリケーションを使用してデータを復元不可能にする必要があります。 *必要ない場合は、保存してはいけません。*

要件とテスト手順		ガイダンス
適用に関する注意事項 アカウントデータが TPSP によって（例えば、クラウド環境で）保管される場合、事業体は、サービスプロバイダと協力して、TPSP がどのように事業体のこの要件を満たすかを理解する責任がある。考慮すべき点は、データ要素のすべての地理的インスタンスが安全に削除されることを保証することである。 *上記の箇条書き（オーソリゼーションの完了前に保存された機密認証データ（SAD）の適用範囲）は、2025 年 3 月 31 日までのベストプラクティスで、それ以降は要件 3.2.1 の一部として要件となり、PCI DSS 評価時に十分に考慮する必要がある。*		**例** 自動化されたプログラム的な手順を実行してデータを探し出し削除することも、データ保存領域の手動レビューを実行することも可能です。いずれの方法を用いるにせよ、プロセスが正常に完了し、結果が記録され、完了したことが検証されていることを確認するために、プロセスを監視することは良い考えです。安全な削除方法を導入することで、不要になったデータを確実に取得できないようにします。 **その他の情報** *NIST SP 800-88 Rev. 1,「媒体のサニタイズに関するガイドライン」*を参照してください。

要件とテスト手順		ガイダンス
3.3 機密認証データ（SAD）は、オーソリゼーション後に保存されない。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.3.1 機密認証データ（SAD）は、暗号化されていても、オーソリゼーション後は保持されない。受信したすべての機密認証データは、オーソリゼーションプロセスが完了した時点で復元不可能になる。	**3.3.1.a** 機密認証データ（SAD） を受信する場合、文書化されたポリシー、手順、およびシステム構成を調べ、データがオーソリゼーション後 に保持されないことを確認する。 **3.3.1.b** 機密認証データ（SAD） を受信する場合、文書化された手順を調べ、安全なデータ削除プロセスを観察し、オーソリゼーションプ ロセスの完了時にデータが復元不可能な状態になることを確認する。	機密認証データ（SAD） は、悪意のある個人にとって、偽造ペイメントカードの生成や不正な取引を可能にするため、非常に価値があります。従って、オーソリゼーションプロセス完了後の 機密認証データ（SAD）の保存は禁止されています。 **定義** 加盟店が取引の応答（承認または拒否など）を受信した時点で、オーソリゼーションプロセスが完了します。
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		
適用に関する注意事項		
この要件は、イシュアおよびイシュイングサービスをサポートする企業（機密認証データ（SAD）が正当なイシュイングビジネスニーズで必要とされる場合）であって、機密認証データを保存するビジネス上の正当性がある場合には適用されない。 イシュア固有の追加要件については、要件 3.3.3 を参照すること。 機密認証データには、要件 3.3.1.1 から要件 3.3.1.3 で引用されるデータが含まれる。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** トラック（カード裏面の磁気ストライプ（存在する場合）、チップなどに含まれる同等のデータ）の全内容が保存されている場合、そのデータを入手した悪意のある者は、ペイメントカードの複製や不正取引の完了にそのデータを使用することが可能です。 **定義** フルトラックデータは、フルトラック、トラック、トラック 1、トラック 2、磁気ストライプデータなどと呼ばれることもあります。各トラックには多くのデータ要素が含まれ、この要件は、オーソリゼーション後に保持される可能性のあるもののみを指定します。 **例** オーソリゼーションプロセスの完了時にトラックの全内容が保持されないことを確認するためにレビューするデータソースは、以下のものが含まれますが、これらに限定されません。 • 受信トランザクションデータ • すべてのログ（例えば、トランザクション、履歴、デバッグ、エラー） • 履歴ファイル • トレース・ファイル • データベーススキーマ *(次ページに続く)*
3.3.1.1 オーソリゼーションプロセスの完了時に、トラックの全内容が保持されない。	**3.3.1.1** データソースを調査し、オーソリゼーションプロセスの完了時にトラックの全内容が保存されていないことを確認する。	
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外である。		
適用に関する注意事項 通常の取引過程では、トラックからの以下のデータ要素を保持する必要が生じる場合がある。 • カード会員名 • プライマリアカウント番号（PAN） • 有効期限 • サービスコード リスクを最小限に抑えるために、取引に必要なデータ要素のみを安全に保存する。		

要件とテスト手順		ガイダンス
		• データベースの内容、オンプレミスおよびクラウドデータストア • すべての既存のメモリ／クラッシュダンプファイル

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.3.1.2 オーソリゼーションプロセス完了時に、カード検証コードを保持しない。	**3.3.1.2** データソースを調査し、オーソリゼーションプロセス完了時にカード検証コードが保存されないことを確認する。	カード検証コードのデータが盗まれると、悪意のある者がインターネットや通信販売・電話注文（MO/TO）などで不正な取引を行う可能性があります。このデータを保存しないことで、漏洩する確率を減らすことができます。 **例** カード検証コードをオーソリゼーション完了前に紙媒体に保存する場合、オーソリゼーション完了後に読み取れないように消去または隠蔽する方法が必要です。コードを読めなくする方法の例としては、はさみでコードを取り除く、適切な不透明で剥がせないマーカーをコードの上に貼る、などがあります。 オーソリゼーションプロセスの完了時にカード検証コードが保持されていないことを確認するためにレビューするデータソースは、以下のものが含まれますが、これらに限定されるものではありません。 • 受信トランザクションデータ • すべてのログ（例えば、トランザクション、履歴、デバッグ、エラー） • 履歴ファイル • トレースファイル • データベーススキーマ • データベースの内容、オンプレミスおよびクラウドデータストア
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		
適用に関する注意事項		
カード検証コードとは、カードを提示しない取引の検証に使用される、ペイメントカードの表面または裏面に印刷された 3 桁または 4 桁の番号のことである。		

要件とテスト手順		ガイダンス
		• すべての既存のメモリ／クラッシュダンプファイル

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.3.1.3 オーソリゼーションプロセスの完了時に 、個人識別番号（PIN）および PIN ブロックを保持しない。	**3.3.1.3** データソースを調査し、オーソリゼーションプロセスの完了時に PIN および PIN ブロックが保存されないことを確認する。	PIN および PIN ブロックは、カードの所有者またはカードを発行した事業体のみが知っている必要があります。このデータが盗まれた場合、悪意のある者が PIN を使った不正な取引（例えば、店舗での買い物や ATM での引き出しなど）を実行する可能性があります。このデータを保存しないことで、漏洩する確率を減らすことができます。 **例** オーソリゼーションプロセスの完了時に PIN および PIN ブロックが保持されていないことを確認するために見直すデータソースは、以下のものが含まれますが、これらに限定されるものではありません。 • 受信トランザクションデータ • すべてのログ（例えば、トランザクション、履歴、デバッグ、エラー） • 履歴ファイル • トレースファイル • データベーススキーマ • データベースの内容、オンプレミスおよびクラウドデータストア • すべての既存のメモリ／クラッシュダンプファイル
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		
適用に関する注意事項		
PIN ブロックは取引プロセスの自然な過程で暗号化されるが、事業体が PIN ブロックを再度暗号化しても、オーソリゼーションプロセスの完了後に保存することはできない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチテスト手順**	**目的**
3.3.2 オーソリゼーションが完了する前に電子的に保存される 機密認証データ（SAD） は、強力な暗号化技術を使用して暗号化される。	**3.3.2** データストア、システム構成、および／またはベンダの文書を調査し、オーソリゼーション完了前に電子的に保存されるすべての 機密認証データ（SAD） が、強力な暗号化技術を使用して暗号化されていることを確認する。	機密認証データ（SAD）は、悪意のある者が偽造ペイメントカードを正常に生成し、不正な取引を行う確率を高めるために使用される可能性があります。
カスタマイズアプローチの目的		**グッドプラクティス**
この要件は、カスタマイズアプローチの対象外である。		事業体は、PAN の暗号化に使用するのとは異なる暗号鍵で 機密認証データ（SAD） を暗号化することを検討すべきです。ただし、機密認証データ（SAD） に含まれる PAN（トラックデータの一部）を別途暗号化する必要があることを意味するものではありません。
適用に関する注意事項		**定義**
オーソリゼーション前の機密認証データ（SAD） の保存が許可されているかどうかは、コンプライアンスプログラムを管理する事業体（例えば、ペイメントブランドやアクワイアラ）によって決定される。追加的な基準については、該当する組織に問い合わせること。 この要件は、環境内に PAN が存在しない場合でも、機密認証データ（SAD） のすべての保存に適用される。		オーソリゼーションプロセスは、オーソリゼーション要求の応答に対する応答（すなわち、承認または拒否）が受信されると即座に完了します。
(次ページに続く)		

要件とテスト手順		ガイダンス
オーソリゼーション完了前に 機密認証データ（SAD） が保存される場合に適用される追加要件については、要件 3.2.1 を参照すること。 この要件は、イシュアおよび 機密認証データ（SAD） を保存することに正当なイシュイング業務上の理由があるイシュイングサービスをサポートする事業体会社には 適用されない。 イシュアに固有の要件については、要件 3.3.3 を参照のこと。 この要件は、PIN ブロックの管理方法を置き換えるものではなく、また適切に暗号化された PIN ブロックを再度暗号化する必要があることを意味するものでもない。 *この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.3.3 ***イシュアおよびイシュイングサービスをサポートし機密認証データを保存する企業に対する追加要件：***機密認証データの保存では • 正当なイシュイング業務に必要なものに限定し、安全性を確保する。 • 強力な暗号化技術を使用して暗号化されていること。*この箇条は、発効日まではベストプラクティスである。詳細については、以下の「適用に関する注意事項」を参照。*	**3.3.3.a** ***イシュアおよびイシュイングサービスをサポートし機密認証データを保存する企業に対する追加のテスト手順：*** 文書化されたポリシーを調査し、担当者にインタビューして、機密認証データの保存に関する文書化されたビジネス上の正当性があることを確認する。	**機密認証データ（SAD）** は、悪意のある者が偽造ペイメントカードの生成に成功し、不正な取引を行う確率を高めるために使用される可能性があります。 **グッドプラクティス** 事業体は、PAN の暗号化に使用するのとは異なる暗号化鍵で 機密認証データ（SAD） を暗号化することを検討すべきです。ただし、機密認証データ（SAD） に含まれる PAN を（トラックデー
カスタマイズアプローチの目的	**3.3.3.b** ***イシュアおよびイシュイングサービスをサポートし機密認証データを保存する企業に対する追加のテスト手順：*** データストアおよびシステム構成を調査し、機密認証データが安全に保管されていることを確認する。	
機密認証データは、イシュイング機能をサポートするために必要な場合にのみ保持され、不正なアクセスから保護される。		

要件とテスト手順		ガイダンス
適用に関する注意事項 この要件は、イシュアおよびイシュイング業務を支援し、機密認証データを保存する企業にのみ適用される。 ペイメントカードを発行する事業体、またはイシュイングサービスを実行もしくは支援する事業体は、多くの場合、イシュイング機能の一部として機密認証データを作成し、管理する。イシュイングサービスを実行、促進、またはサポートする企業が機密認証データを保存することは、そのようなデータを保存する正当なビジネスニーズがある場合にのみ許容される。 PCI DSS の要件は、イシュアを含め、 アカウントデータを保存、処理、または伝送するすべての事業体を対象としている。イシュアおよびイシュアプロセサーの唯一の例外は、正当な理由がある場合に機密認証データを保持できることである。このようなデータはすべて、PCI DSS および特定のペイメントブランドの要件に従って安全に保存されなければならない。 *上記の箇条書き（保存された 機密認証データ（SAD） を強力な暗号化技術で暗号化する）は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は要件 3.3.3 の一部として要件となり、PCI DSS 評価中に十分に考慮する必要がある。*		タの一部として）別途暗号化する必要があることを意味するものではありません。 **定義** 正当なイシュイング業務上の必要性とは、イシュイング業務プロセスを促進するためにデータが必要であることを意味します。 **その他の情報** *ISO/DIS 9564-5 金融サービス - 個人識別番号（PIN）管理およびセキュリティ - パート 5 を参照のこと。高度な暗号化規格を使用した PIN およびカードセキュリティデータの生成、変更、検証方法。*

要件とテスト手順		ガイダンス
3.4 PAN 全体 の表示へのアクセス、および PAN のコピー機能が制限されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.4.1 PAN は表示時にマスクされ（BIN と末尾 4 桁が**最大表示桁数**）、業務上の正当な理由のある担当者のみが BIN と PAN の末尾 4 桁**より多く**見ることができる。	**3.4.1.a** PAN の表示をマスキングするための文書化されたポリシーと手順を調べ、以下を確認する。 • BIN と PAN の末尾 4 桁より多く（PAN 全体を含む）のアクセス権を必要とする役割のリストが、各役割がそのようなアクセス権を持つための正当なビジネス上の必要性とともに文書化されている。 • PAN は表示時にマスクされ、正当な業務上の必要性を有する担当者のみが BIN および PAN の末尾 4 桁より多くを見ることができるようにする。 • PAN 全体の表示を特に許可されていないすべての役割では、マスクされた PAN のみを表示しなければならない。	コンピュータ画面、ペイメントカードのレシート、紙の報告書などに PAN 全体 が表示されると、このデータが不正に取得され、不正に使用される可能性があります。PAN 全体 が正当な業務上の必要性を持つ者にのみ表示されるようにすることで、不正な者が PAN データにアクセスするリスクを最小限に抑えることができます。
カスタマイズアプローチの目的		**グッドプラクティス**
PAN の表示は、定義されたビジネスニーズを満たすために必要な最小限の桁数に制限される。		定義された役割に応じたアクセス制御を適用することは、PAN 全体の表示のアクセスを、定義されたビジネスニーズを持つ個人のみに制限する 1 つの方法です。 マスキングの方法は、特定のビジネス機能を実行するために必要な桁数のみを常に表示する必要があります。例えば、あるビジネス機能を実行するために末尾 4 桁だけが必要な場合、PAN は末尾 4 桁だけを表示するようにマスキングする必要があります。別の例として、ある機能がルーティング目的で銀行識別番号（BIN）を表示する必要がある場合、その機能の BIN 桁のみをアンマスクします。
適用に関する注意事項	**3.4.1.b** システム構成を調査し、PAN 全体が表示されるのは文書化されたビジネスニーズを持つ役割に限られ、それ以外の要求には PAN がマスクされていることを確認する。	
この要件は、カード会員データの表示に関するより厳しい要件（POS 領収書に関する法的要件またはペイメント ブランド要件など）に取って代わるものではありません。 *(次ページに続く)*		*(次ページに続く)*

要件とテスト手順		ガイダンス
この要件は、画面、紙の領収書、印刷物などに表示される PAN の保護に関するものであり、保存、処理、伝送される PAN の保護に関する要件 3.5.1 と混同しないようにする必要がある。	**3.4.1.c** PAN の表示（画面や紙の領収書など）を調査し、PAN が表示されるときにマスクされていること、また、正当な業務上の必要性がある人だけが BIN および／または PAN の末尾 4 桁より多くを見ることができることを確認する。	**定義** マスキングはトランケーションと同義ではなく、これらの用語を同じように使うことはできません。マスキングとは、PAN 全体がシステムに保存されている場合でも、表示または印刷時に特定の桁を隠すことを指します。これは、切り捨てられた桁が削除され、システム内で検索できないようにするトランケーションとは異なります。マスクされた PAN は「アンマスク」できるが、別のソースから PAN を再作成しない限り「アントランケート」することはできません。 **その他の情報** マスキングとトランケーションの詳細については、これらのトピックに関する PCI SSC の FAQ を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.4.2 リモートアクセステクノロジを使用する場合、技術的なコントロールにより、文書化された明示的な承認と正当かつ定義されたビジネスニーズを持つ者を除き、すべての担当者の PAN のコピーおよび／または移動を防止する。	**3.4.2.a** リモートアクセステクノロジを使用する際に、PAN をローカルのハードドライブまたはリムーバブル電子媒体にコピーおよび／または移動することを防止する技術的なコントロールについて、文書化したポリシーおよび手順、文書化した証拠を調べ、以下を確認する。 • 技術的なコントロールにより、特に許可されていないすべての担当者が PAN をコピーおよび／または移動することを防止している。 • PAN のコピーおよび／または移動を許可された担当者のリストが、文書化された明示的な権限および正当かつ定義されたビジネスニーズとともに維持されている。	PAN を不正な記憶装置に移動することは、このデータを入手し不正に使用するための一般的な方法です。 明確な権限を持ち、正当なビジネス上の理由がある者だけが PAN をコピーまたは移動できるようにすることで、権限のない者が PAN にアクセスするリスクを最小限に抑えることができます。
カスタマイズアプローチの目的		**グッドプラクティス**
権限のない担当者がリモートアクセステクノロジを使用して、PAN をコピーしたり移動したりすることはできない。		PAN のコピーと移動は、その個人に対して許容され、許可されたストレージデバイスにのみ行うべきです。
適用に関する注意事項	**3.4.2.b** リモートアクセステクノロジの構成を調査し、明示的に許可された場合を除き、すべての担当者に対して PAN のコピーや移動を防止するための技術的なコントロールが行われていることを確認する。	**定義**
ローカルハードディスク、リムーバブル電子媒体、およびその他のストレージデバイスに PAN を保存または移動すると、これらのデバイスが PCI DSS の適用範囲に含まれることになる。 *この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*	**3.4.2.c** プロセスを観察し、担当者にインタビューして、リモートアクセステクノロジを使用する場合、文書化された明確な権限と、正当で定義されたビジネスニーズを持つ担当者のみが、PAN のコピーおよび／または移動の許可のあることを確認する。	仮想デスクトップは、リモートアクセステクノロジの一例ですあ。 ストレージデバイスには、ローカルハードディスク、仮想ドライブ、リムーバブル電子媒体、ネットワークドライブ、クラウドストレージが含まれるが、これらに限定されません。
		その他の情報
		使用されているリモートアクセステクノロジのベンダ文書には、この要件を実装するために必要なシステム設定に関する情報が記載されています。

要件とテスト手順		ガイダンス
3.5 プライマリアカウント番号（PAN）は、保存場所に関わらず、保護されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.5.1 PAN は、以下のいずれかの方法を用いて、保存されている場所の読み取りを不可能にする。 • 強力な暗号化技術に基づく PAN 全体の一方向ハッシュ • トランケーション（PAN の切り捨てられたセグメントをハッシュで置き換えることはできない） – 同じ PAN をハッシュ化したものと切り捨てたもの、あるいは同じ PAN を異なる形式で切り捨てたものが環境内に存在する場合、異なるバージョンを関連付けて元の PAN を復元できないようにするための追加的なコントロールが行われる。 • インデックストークン • 強力な暗号化技術と、関連する鍵管理プロセスおよび手順。	**3.5.1.a** PAN を読み取り不能にするために使用したシステムに関する文書（ベンダ、システム／プロセスのタイプ、（該当する場合は）暗号化アル ゴリズムなど）を調査し、この要件で指定されたいずれかの方法で PAN が読み取り不能にされたことを確認する。 **3.5.1.b** データリポジトリと監査ログ（決済アプリケーションのログを含む）を調査し、この要件で指定され たいずれかの方法を使用して PAN が読み取り不能になったことを確認する。 **3.5.1.c** 同じ PAN のハッシュ化されたバージョンと切り捨てられたバージョンが環境に存在する場合、実装されたコントロールを調べ、ハッシュ化されたバージョンと切り捨てられたバージョンが元の PAN を再構築するために関連付けられないことを確認する。	平文で保存された PAN を除去することは、事業体の一次的なアクセス制御の脆弱性または設定ミスを利用して、権限のない個人が保存データにアクセスした場合にデータを保護するために設計された多層防御です。 二次的な独立した制御システム（例えば、暗号化鍵や復号鍵へのアクセスや使用を管理する）により、一次的なアクセス制御システムの障害による PAN の機密性の侵害を防ぐことができます。保存されている平文 PAN の除去にハッシュを使用した場合、ハッシュ化されたバージョンと切り捨てられたバージョンの PAN を関連付けると、悪意のある者は元の PAN 値を容易に導き出すことが可能です。このデータの相関を防ぐには、オリジナルの PAN を読み取り不能に維持することが有効です。
カスタマイズアプローチの目的		**その他の情報**
記憶媒体から平文の PAN を読み取ることができない。		トランケーションのフォーマットとトランケーション全般に関する情報は、PCI SSC の FAQ を参照してください。 インデックストークンに関する情報源は以下の通りです。
(次ページに続く)		*(次ページに続く)*

要件とテスト手順		ガイダンス
適用に関する注意事項 悪意のある者が、PAN のトランケートされたバージョンとハッシュ化されたバージョンの両方にアクセスできれば、オリジナルの PAN データを再構築するのは比較的簡単な作業である。 この要件は、主な保管場所（データベース、テキストファイルやスプレッドシートなどのフラットファイル）に保存された PAN と、それ以外の保管場所（バックアップ、監査ログ、例外ログ、トラブルシューティングログ）に保存された PAN のいずれにも適用され、すべて保護する必要がある。 この要件は、PAN の暗号化および復号の際に、平文の PAN を含む一時ファイルを使用することを妨げるものではない。		• PCI SSC のトークン化製品セキュリティガイドライン (*https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf*) • *ANSI X9.119-2-2017:小売金融サービス - 機密性の高いペイメントカードデータの保護に関する要件 - パート 2:オーソリゼーション後トークン化システムの実装*

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 平文で保存された PAN を除去することは、事業体の一次的なアクセス制御の脆弱性または設定ミスを利用して、権限のない個人が保存データにアクセスした場合にデータを保護するために設計された多層防御です。 二次的な独立した制御システム（例えば、暗号化鍵および復号鍵のアクセスや使用を管理する）により、一次的なアクセス制御システムの障害による PAN の機密性の侵害を防ぐことができます。 **グッドプラクティス** ランダムに生成される秘密鍵を組み込んだハッシュ関数により、ブルートフォース攻撃への耐性と秘密認証の完全性を実現します。 **その他の情報** 適切な鍵付き暗号化ハッシュアルゴリズムには、HMAC、CMAC、GMAC が含まれますが、これらに限定されるものではありません。有効な暗号強度は少なくとも 128 ビットです（*NIST SP 800-131Ar2*）。 *(次ページに続く)*
3.5.1.1 PAN を読み取り不能にするために使用するハッシュ（要件 3.5.1 の最初の箇条書きによる）は、PAN 全体の鍵付き暗号ハッシュであり、要件 3.6 および 3.7 に従った関連鍵管理プロセスおよび手順と関連付けられている。	**3.5.1.1.a** PAN を読み取り不能にするために使用されたハッシュ法について、ベンダ、システム／プロセスのタイプ、暗号化アル ゴリズム（該当する場合）を含む文書を調査し、ハッシュ法が PAN 全体の鍵付き暗号ハッシュとなり、鍵管理プロセスおよび手 続きと関連付けられていることを確認する。	
適用に関する注意事項	**3.5.1.1.b** 鍵付き暗号化ハッシュに関連する鍵管理手順およびプロセスに関する文書を調査し、要件 3.6 および 3.7 に従って鍵が管理されていることを確認する。	
この要件は、主な保管場所（データベース、またはテキストファイル・スプレッドシートなどのフラットファイル）に保存されている PAN と、それ以外の保管場所（バックアップ、監査ログ、例外、トラブルシューティングログ）に保存された PAN のいずれにも適用され、すべて保護する必要がある。 この要件は、PAN の暗号化および復号の際に、平文の PAN を含む一時ファイルを使用することを妨げるものではない。 *この要件は、2025 年 3 月 31 日まではベストプラクティスとみなされ、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*	**3.5.1.1.c** データリポジトリを調査し、PAN が読み取り不能になっていることを確認する。	

要件とテスト手順		ガイダンス
	3.5.1.1.d 決済アプリケーションのログを含む監査ログを調査し、PAN が読み取り不能になっていることを確認する。	HMAC、CMAC、GMAC の詳細については、それぞれ以下を参照してください。*NIST SP 800-107r1*、*NIST SP 800-38B*、*NIST SP 800-38D*）。 *NIST SP 800-107 (Revision 1)：承認されたハッシュアルゴリズムを使用するアプリケーションの推奨事項*§5.3 を参照してください。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.5.1.2 ディスクレベルまたはパーティションレベルの暗号化（ファイル、列、フィールドレベルのデータベース暗号化ではない）を使用して PAN を読み取り不能にする場合、以下のようにのみ実装される。 • リムーバブル電子メディア上 **または** • リムーバブルでない電子メディアに使用する場合は、要件 3.5.1 を満たす別のメカニズムで PAN も読み取り不能にする。	**3.5.1.2.a** 暗号化プロセスを調査し、ディスクレベルまたはパーティションレベルの暗号化で PAN を読み取り不能にする場合、以下のようにのみ実装されていることを確認する。 • リムーバブル電子メディア上 **または** • リムーバブルでない電子メディアに使用する場合は、使用する暗号化プロセスを調べ、要件 3.5.1 を満たす別の方法でも PAN を読み取り不能にしていることを確認する。	ディスクレベルおよびパーティションレベルの暗号化では、通常、同じキーを使用してディスクまたはパーティション全体を暗号化し、システムの実行時または許可されたユーザの要求時にすべてのデータが自動的に復号されます。このため、ディスクレベルの暗号化は、コンピュータ、ラップトップ、サーバ、ストレージアレイ、その他ユーザ認証によって透過的に復号されるシステム上の保存された PAN を保護するには適切ではありません。 **その他の情報** 利用可能な場合、ベンダのハードニングおよび業界のベストプラクティスのガイドラインに従うことで、これらのデバイス上の PAN を保護することができます。
カスタマイズアプローチの目的	**3.5.1.2.b** 構成および／またはベンダのドキュメントを調べ、暗号化プロセスを観察し、システムがベンダのドキュメントに従って構成され、ディスクまたはパーティションが読み取り不能になっていることを確認する。	
この要件は、カスタマイズアプローチの対象外である。 *(次ページに続く)*		

要件とテスト手順		ガイダンス
適用に関する注意事項		
これらのタイプのデバイスにはディスク暗号化が引き続き存在する可能性があるが、これらのシステムに保存された PAN を保護するために使用されるメカニズムはそれだけではない。保存された PAN は、要件 3.5.1 に従って、例えば、トランケーションやデータレベルの暗号化メカニズムによっても読み取り不能にする必要がある。フルディスク暗号化は、ディスクが紛失した場合にデータを保護するのに役立つため、リムーバブル電子メディアストレージデバイスにのみ使用することが適切である。 データセンタのアーキテクチャの一部であるメディア（ホットスワップ可能なドライブ、バルクテープバックアップなど）は、要件 3.5.1 が適用される非リムーバブル電子メディアとみなされる。 ディスクまたはパーティションの暗号化実装は、他のすべての PCI DSS 暗号化および鍵管理要件も満たす必要がある。 *この要件は 2025 年 3 月 31 日まではベストプラクティスであるが、それ以降は必須となるため、PCI DSS 評価中に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.5.1.3 PAN を読み取り不能にするために、（ファイル、列、フィールドレベルのデータベース暗号化ではなく、）ディスクレベルまたはパーティションレベルの暗号化を使用する場合、次のように管理する。 • 論理アクセスは、ネイティブのオペレーティングシステムの認証およびアクセス制御メカニズムとは別に、独立して管理する。 • 復号鍵はユーザアカウントと関連付けない。 • 暗号化されていないデータへのアクセスを許可する認証要素（パスワード、パスフレーズ、暗号鍵）は、安全に保管されます。	**3.5.1.3.a** ディスクレベルまたはパーティションレベルの暗号化を使用して PAN を読み取り不能にする場合、システム構成を調べ、認証プロセスを観察して、論理アクセスがこの要件で指定されたすべての要素に従って実装されていることを確認する。	ディスクレベルの暗号化は、通常、同じ鍵を使用してディスクまたはパーティション全体を暗号化し、システムの実行時または許可されたユーザからの要求時にすべてのデータを自動的に復号します。多くのディスク暗号化ソリューションは、オペレーティングシステムの読み取り／書き込み操作を傍受し、システム起動時またはセッション開始時にパスワードまたはパスフレーズを入力する以外、ユーザが特別な操作をしなくても適切な暗号化変換を実行します。これは、有効なユーザアカウントへのアクセスを既に取得している悪意のある者に対して無防備です。
カスタマイズアプローチの目的	**3.5.1.3.b** 認証要素（パスワード、パスフレーズ、暗号鍵）を含むファイルを調査し、担当者にインタビューを行い、暗号化されていないデータへのアクセスを許可する認証要素が安全に保管され、ネイティブオペレーティングシステムの認証およびアクセス制御方法から独立していることを確認します。	**グッドプラクティス**
ディスク暗号化の実装は、復号のために独立した認証と論理アクセス制御を必要とするように構成されている。		フルディスク暗号化は、ディスクの紛失時にデータを保護するのに役立つので、その使用はリムーバブル電子メディアストレージデバイスにのみ限定するのが最適です。
適用に関する注意事項		
ディスクまたはパーティションの暗号化実装は、他のすべての PCI DSS 暗号化および鍵管理要件も満たす必要がある。		

要件とテスト手順		ガイダンス
3.6 保存されているアカウントデータを保護するために使用される暗号化鍵が保護されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 暗号化鍵は、アクセス権を取得した者がデータを復号することができるため、強力に保護する必要があります。 **グッドプラクティス** 暗号化鍵の管理は、業界標準の集中型鍵管理システムを使用することが推奨されます。 **その他の情報** 事業体の鍵管理手順は、業界の要件に合わせることでメリットがあります。暗号化鍵管理のライフサイクルに関する情報源には以下のものがあります。 • *ISO 11568-1 バンキング- キーマネージメント（小売）- パート 1* 原則(特に第 10 章および参照される第 2 部および第 4 部) • *-NIST SP 800-57 パート 1 リビジョン 5- 鍵管理に関する推奨事項、パート 1:。一般*
3.6.1 保存されたアカウントデータを開示や誤用から保護するために使用される暗号鍵を保護するため、以下のような手順が定義され、実施される。 • 暗号化鍵へのアクセスが必要最小限の管理者に制限されている。 • 鍵暗号化鍵が少なくとも保護対象データの暗号化鍵と同じ強度を有する。 • 鍵暗号化鍵は、データ暗号化鍵とは別に保存される。 • 鍵の保存場所と形式を最小限にし、安全に保存する。	**3.6.1** 文書化された鍵管理ポリシおよび手順を調査し、保存されたアカウントデータを開示および誤用から保護するために使用される暗号化鍵を保護するプロセスが、この要件で指定されたすべての要素を含むように定義されていることを確認する。	
カスタマイズアプローチの目的		
保存されたアカウントデータを開示や誤用から保護するために使用される暗号化鍵を保護するプロセスが定義され、実装されている。		
(次ページに続く)		

要件とテスト手順		ガイダンス
適用に関する注意事項		
この要件は、アカウントデータの暗号化に使用される鍵、およびデータ暗号化鍵を保護するために使用される鍵暗号化鍵に適用される。 保存されたアカウントデータを保護するために使用される鍵を開示や誤用から保護するという要 件は、データ暗号化鍵と鍵暗号化鍵の双方に適用される。1 つの鍵暗号化鍵が多くのデータ暗号化鍵へのアクセスを可能にするため、鍵暗号化鍵には強力な保護対策が必要となる。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.6.1.1 ***サービスプロバイダのみに対する追加要件:*** 暗号化アーキテクチャについて、以下を含む文書化された記述が維持されている。 • 保存されたアカウントデータの保護に使用される全てのアルゴリズム、プロトコルおよび鍵の詳細（鍵の強度および有効期限を含む） • 本番環境とテスト環境で同じ暗号化鍵が使用されないようにすること。*この箇条は発効日までのベストプラクティスであり、詳細は下記の適用に関する注意事項を参照すること* • 各鍵の使用方法の説明 • 要件 12.3.4 に示すように、鍵管理に使用されるハードウェアセキュリティモジュール（HSM）、鍵管理システム （KMS）、その他の安全な暗号化装置（SCD）のインベントリ（装置の種類と場所を含む）	**3.6.1.1** ***サービスプロバイダ評価のみの追加テスト手順：*** 責任者にインタビューを行い、文書を調査して、本要件で指定されたすべての要素を含む暗号化アーキテクチャを説明する文書が存在することを確認する。	暗号化アーキテクチャの最新の文書を維持することにより、事業体は、保存されたアカウントデータを保護するために使用されるアルゴリズム、プロトコル、暗号鍵、および鍵を生成、使用、保護するデバイスを理解することができます。これにより、事業体は、その暗号化アーキテクチャに対する脅威の進展に対応し、異なるアルゴリズ ムや鍵の強度が提供する保証レベルの変化に応じて、更新を計画することができます。また、このような文書を維持することにより、事業体は鍵や鍵管理デバイスの紛失や欠落を検知し、暗号アーキテクチャへの未承認の追加を特定することができます。 本番環境とテスト環境の両方で同じ暗号化鍵を使用することは、テスト環境が本番環境と同じセキュリ ティ・レベルでない場合、鍵が漏洩するリスクをもたらします。 **グッドプラクティス** 自動報告メカニズムを持つことで、暗号化属性の保守を支援することができます。
カスタマイズアプローチの目的 暗号化アーキテクチャの正確な詳細が維持され、利用可能である。		

(次ページに続く)

要件とテスト手順		ガイダンス
適用に関する注意事項 この要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用される。 クラウド HSM の実装では、本要件に従った暗号アーキテクチャの責任は、クラウドプロバイダとクラウド顧客の間で共有される。 *上記の箇条書き（本番環境とテスト環境で同じ暗号鍵を使用しないことを暗号化アーキテクチャに含める）は、2025 年 3 月 31 日まではベストプラクティスである。2025 年 3 月 31 日以降は要件 3.6.1.1 の一部として要件となり、PCI DSS 評価中に十分に考慮する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.6.1.2 保存されているアカウントデータの暗号化・復号に使用する秘密鍵（共通鍵暗号）およびプライベート鍵（公開鍵暗号）は、常に次のいずれか（複数可）の形態で保存される。 • データ暗号化鍵と同等以上の強度を持つ鍵暗号化鍵で暗号化され、データ暗号化鍵とは別に保管される。 • ハードウェア・セキュリティ・モジュール（HSM）や PTS が承認した加盟店端末などの安全な暗号化デバイス（SCD）内にあること • 業界で認められた方法に従い、少なくとも 2 つのフルレングスの鍵コンポーネントまたは鍵共有として	**3.6.1.2.a** 文書化された手順を調査し、保存されたアカウントデータの暗号化／復号に使用される暗号化鍵は、本要件で指定されたうちのいずれか（複数可）の形式でのみ存在しなければならないと定義されていることを確認する。	暗号化鍵を安全に保管することで、不正アクセスや不必要なアクセスを防ぎ、保管されているアカウントデータの漏洩を防ぎます。鍵を別々に保管することは、1 つ目の鍵の所在が漏洩しても、2 つ目の鍵が漏洩しないように保管することです。
	3.6.1.2.b システム構成および鍵の保管場所を調査し、保存されているアカウントデータの暗号化／復号に使用される暗号化鍵が、本要件で指定される いずれか（複数可）の形式で存在することを確認する。	**グッドプラクティス**
カスタマイズアプローチの目的	**3.6.1.2.c** 鍵暗号化鍵が使用されている場合は必ず、システム構成および鍵の保管場所を調査し、以下を確認する。 • 鍵暗号化鍵は、少なくとも、保護するデータ暗号化鍵と同程度の強度を有する。 • 鍵暗号化鍵は、データ暗号化鍵とは別に保管される。	データ暗号鍵が HSM に保管されている場合、HSM との通信チャネルは、暗号化または復号化の 操作が傍受されないように保護されるべきです。
秘密鍵およびプライベート鍵は、不正な取得やアクセスを防止する安全な形態で保管される。		

要件とテスト手順		ガイダンス
適用に関する注意事項 公開鍵は、これらのいずれかの形式で保管されることを要しない。 SCD を使用する鍵管理システム（KMS）の一部として保管される暗号化鍵は許容される。 暗号化鍵が 2 つに分割されている場合は、この要件を満たさない。鍵コンポーネントまたは鍵共有として保管される秘密鍵またはプライベート鍵は、以下のいずれかの方法で生成されなければならない。 • 承認された乱数発生器を使用し、SCD 内で生成する。 **または** • 秘密鍵共有の生成に関する ISO19592 または同等の業界標準に準拠する。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.6.1.3 平文の暗号化鍵コンポーネントへのアクセスは、必要最小限の管理者に制限される。	**3.6.1.3** ユーザのアクセスリストを調査し、平文の暗号化鍵コンポーネントへのアクセスが必要最小限の管理者に制限されていることを確認する。	平文の暗号鍵コンポーネントにアクセスできる人数を制限することで、保存されているアカウントデータが不正に取得されたり、可視化されたりするリスクを低減することができます。 **グッドプラクティス** 定義された鍵の管理責任（暗号化鍵の作成、変更、ローテーション、配布、その他の方法での保守）を持つ担当者のみに、鍵コン ポーネントへのアクセス権を与えるべきです。 理想的には、これはごく少数の担当者に限定されます。
カスタマイズアプローチの目的		
暗号化鍵コンポーネントへのアクセスは必要な担当者に制限されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.6.1.4 暗号化鍵は、可能な限り少ない場所に保管される。	**3.6.1.4** 鍵の保管場所を調査し、プロセスを観察して、鍵が可能な限り少ない場所に保管されていることを確認する。	あらゆる暗号化鍵を最小限に保管することは、組織がすべての鍵の場所を追跡、監視することを助け、鍵が権限のない第三者にさらされる可能性を最小限に抑えます。
カスタマイズアプローチの目的		
暗号化鍵は必要な場合のみ保持されている。		

要件とテスト手順		ガイダンス
3.7 保存されているアカウントデータを保護するために暗号が使用されている場合、鍵のライフサイクルのすべての側面を網羅する鍵管理プロセスおよび手順が定義され、実施されている。		
定義されたアプローチの要件 **3.7.1** 保存されているアカウントデータの保護に使用される強力な暗号化鍵の生成を含む、鍵管理ポリシおよび手順が実施される。 **カスタマイズアプローチの目的** 強力な暗号化鍵が生成されている。	**定義されたアプローチのテスト手順** **3.7.1.a** 保存されたアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシーおよび手順を調査し、それらが強力な暗号化鍵の生成を定義していることを確認する。 **3.7.1.b** 鍵の生成方法を観察し、強力な鍵が生成されていることを確認する。	**目的** 強力な暗号化鍵の使用は、暗号化されたアカウントデータのセキュリティレベルを大幅に向上させます。 **その他の情報** 付録 G の暗号化鍵の生成で参照されているソースを参照してください。
定義されたアプローチの要件 **3.7.2** 保存されているアカウントデータの保護に使用される暗号化鍵の安全な配布を含む、鍵管理ポリシおよび手順が実施されている。 **カスタマイズアプローチの目的** 暗号化鍵の配布時に安全が確保されている。	**定義されたアプローチのテスト手順** **3.7.2.a** 保存されたアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシーおよび手順を調査し、暗号化鍵の安全な配 布を定義していることを確認する。 **3.7.2.b** 鍵の配布方法を観察し、鍵が安全に配布されていることを確認する。	**目的** 秘密鍵（共通鍵暗号）またはプライベート鍵（公開鍵暗号）の安全な配布または伝達とは、鍵が要件 3.6.1.2 で特定される許可された管理者にのみ配布され、決して安全でない配布は行われないことを意味します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 鍵の保護が不十分なまま保管すると、攻撃者にアクセスされ、復号化されてアカウントデータが流出する可能性があります。 **グッドプラクティス** データ暗号化鍵は、鍵暗号化鍵で暗号化することにより保護することができます。 鍵は、HSM（ハードウェアセキュリティモジュール）に保存することができます。 データを復号することができる秘密鍵またはプライベート鍵は、決してソースコード内に存在させてはなりません。
3.7.3 保管されているアカウントデータの保護に使用される暗号化鍵の安全な保管を含む、鍵管理のポリシーと手順が実装されている。	**3.7.3.a** 保存されたアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシおよび手順を調べ、それらが暗号化鍵の安全な保管を定義していることを確認する。	
	3.7.3.b 鍵の保管方法を観察し、鍵が安全に保管されていることを確認する。	
カスタマイズアプローチの目的 暗号化鍵は保管時に安全が確保されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 暗号期間が終了したら、暗号化鍵を変更することは、誰かが暗号化鍵を入手してデータを復号するリスクを最小化するために不可欠です。 **定義** 暗号期間とは、暗号化鍵が定義された目的に使用できる期間のことです。暗号期間は、鍵が有効である期間および／または鍵によって生成された暗号文の量という観点から定義されることが多くあります。 *(次ページに続く)*
3.7.4 鍵管理のポリシーおよび手順が、関連するアプリケーションベンダまたは鍵の所有者によって定義され、以下を含む業界のベストプラクティスおよびガイドラインに基づき、暗号期間の終わりに達した鍵の変更について実装されている。 • 使用中の鍵タイプごとに定義された暗号期間 • 定義された暗号期間の終了時に鍵を変更するためのプロセス *(次ページに続く)*	**3.7.4.a** 保存されているアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシーおよび手順を調査し、暗号期間が終了した暗号鍵の変更を定義し、この要件で指定されているすべての要素を含むことを確認する。	
	3.7.4.b 鍵が定義された暗号期間の終了時に変更されることを確認するために、担当者にインタビューを行い、文書を調査し、鍵の保管場所を観察する。	

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 暗号化鍵が、定められた暗号期間を超えて使用されていないこと。		暗号期間を定義する際に考慮すべき点は、基礎となるアルゴリズムの強度、 鍵のサイズまたは長さ、鍵の侵害リスク、暗号化されるデータの機密性などが含まれますが、 これらに限定されるものではありません。 **その他の情報** *NIST SP800-57 パート 1、リビジョン 5、セクション 5.3 暗号期間* 特定の鍵が正当な事業体による使用を許可される期間、または特定のシステム用の鍵が有効であり続ける期間を定めるためのガイダンスを提供するものです。鍵の種類に応じた推奨暗号期間については、*SP 800-57* パート 1 の表 1 を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
3.7.5 鍵管理ポリシーおよび手続きは、以下の場合に必要であり、保存されたアカウントデータの保護に使用される鍵の廃止、交換、または破棄を含めて実装される。 • 鍵が、定義された暗号期間の終わりに達した場合 • 鍵の完全性が弱まった場合。これには、平文の鍵コンポーネントを知っている担当者が退社した場合、または鍵コンポーネントを知る役割を終えた場合が含まれる。 • 鍵の漏洩が疑われる、または判明している。 廃止または交換された鍵は、暗号化操作に使用されない。	**3.7.5.a** 保存されたアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシーおよび手順を調査し、本要件で指定されるすべての要素に従い、鍵の廃止、交換、破棄を定義していることを確認する。 **3.7.5.b** 担当者にインタビュを行い、この要件で指定されたすべての要素に従ってプロセスが実装されていることを確認する。	**目的** 不要になった鍵、完全性が損なわれた鍵、漏洩が判明した鍵、または漏洩が疑われる鍵は、アーカイブ、失効、破棄などをして、鍵が使用できなくなるようにしなければなりません。 そのような鍵を保管する必要がある場合（たとえば、アーカイブされた暗号化データをサポートするために）、それらは強力に保護する必要があります。 **グッドプラクティス** アーカイブされた暗号化鍵は、復号化／検証の目的のみに使用さる必要があります。 暗号化ソリューションは、交換時期が到来した鍵、または漏洩が判明した鍵、もしくは漏洩が疑われる鍵を交換するプロセスを提供し、促進する必要があります。さらに、漏洩したことが判明した、または漏洩の疑いがある鍵は、要件 12.10.1 に基づく事業体のインシデント対応計画に従って管理されなければなりません。 **その他の情報** 破棄された鍵をアーカイブするための業界のベストプラクティスは、*NIST SP 800-57 パート 1、リビジョン 5、セクション 8.3.1* に概説されており、信頼できる第三者によるアーカイブの維持と、 アーカイブした鍵情報を運用データとは別に保存することが含まれています。
カスタマイズアプローチの目的		
鍵の完全性が損なわれていることが疑われる場合または判明した場合、鍵は積極的な使用から除去される。		
適用に関する注意事項		
破棄または交換された暗号鍵を保持する必要がある場合、これらの鍵は安全にアーカイブされなければならない（たとえば、鍵暗号化鍵を使用するなど）。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
3.7.6 手動による平文の暗号化鍵の管理操作が担当者によって行われる場合、鍵管理ポリシおよび手順には、知識分割およびデュアルコントロールを使用してこれらの操作を管理することが含まれている。	**3.7.6.a** 保存されているアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシーおよび手順を調査し、それらが知識分割およびデュアルコントロールの使用を定義していることを確認する。 **3.7.6.b** 担当者へのインタビュー、および／またはプロセスの観察により、手動の平文暗号化鍵が知識分割およびデュアルコントロールで管理されていることを確認する。	**目的** 鍵の知識分割とデュアルコントロールは、1 人が鍵全体へのアクセスを行い、データへの不正なアクセス権を取得する可能性を排除するために行われるものです。 **定義** 知識分割とは、2 人以上の人が別々に鍵コンポーネントを持ち、各人が自分の鍵コンポーネントのみを知り、個々の鍵コンポーネントは他のコンポーネントや元の暗号化鍵の知識を伝えない方法です。 デュアルコントロールは、2 人以上の人が暗号鍵の使用を認証するか、鍵管理機能を実行することを必要とします。1 人が他の人の認証要素（パスワード、PIN、鍵など）にアクセスしたり使用したりすることはできません。 **グッドプラクティス** 鍵コンポーネントまたは鍵共有が使用される場合、手順は、1 人の管理者が、暗号化鍵を再構築するのに十分な鍵コンポーネントまたは鍵共有にアクセスできないようにする必要があります。例えば、m-of-n 方式（シャミアの秘密分散法など）では、暗号鍵の再構成に必要な 3 つのコンポーネントのうち 2 つだけが必要とされますが、管理者は 2 つ以上のコンポーネントについて現在または過去に知っていてはなりません。管理者が以前コ
カスタマイズアプローチの目的		
平文の秘密鍵やプライベート鍵は誰にも知られてはならない。平文の鍵に関わる作業は、1 人で行うことはできない。		
適用に関する注意事項		
このコントロールは，手動による鍵管理操作，または暗号化製品によって鍵管理が制御されていない場合に適用される。 単純に 2 つに分割された暗号鍵は、本要件を満たさない。鍵コンポーネントまたは鍵共有として保管される秘密鍵またはプライベート鍵は、以下のいずれかの方法で生成されなければならない。 • 承認された乱数発生器を使用し、ハードウェア・セキュリティ・モジュール（HSM）またはPTS 承認の加盟店端末（ポイント・オブ・インタラクションデバイス）などの安全な暗号化デバイス（SCD）内で生成される。		

要件とテスト手順		ガイダンス
または • 秘密鍵共有の生成に関する ISO19592 または同等の業界標準に準拠する。		ンポーネント A を割り当てられ、その後再割り当てされた場合、その管理者にコンポーネント B または C を割り当ててはなりません。管理者に 2 つのコンポーネントに関する知識とキーを再作成する能力を与えることになるからです。 **例** 手動で行う可能性のある鍵管理操作には、鍵の生成、送信、読み込み、保管、破棄が含まれますが、これらに限定されません。 **その他の情報** 鍵コンポーネントを管理するための業界標準には、以下のようなものがあります。 • *NIST SP 800-57* パート 2、リビジョン 1 --鍵管理に関する推奨事項、パート 2-鍵管理組織のベストプラクティス[4.6 鍵情報の配布]。 • *ISO 11568-2 バンキング– 鍵管理（リテール）-第 2 部:* 対称型暗号、その鍵管理およびライフサイクル [4.7.2.3 鍵コンポーネントと 4.9.3 鍵コンポーネント]. • *欧州ペイメント評議会 EPC342-08 暗号アルゴリズムの使用と鍵管理に関するガイドライン* [特に 4.1.4 鍵のインストール]。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
3.7.7 暗号化鍵の不正置換の防止を含む鍵管理ポリシーおよび手順が実施されている。	**3.7.7.a** 保存されているアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシーおよび手順を調査し、暗号化鍵の不正置換の防止を定義していることを確認する。 **3.7.7.b** 鍵の不正置換え防止されていることを確認するために、担当者にインタビューおよび／またはプロセスを観察する。	攻撃者がある事業体の鍵を、攻撃者が知っている鍵で置き換えることができた場合、攻撃者はその鍵で 暗号化されたすべてのデータを復号することができるようになります。 **グッドプラクティス** 暗号化ソリューションは、未許可のソースまたは予期しないプロセスからの鍵の置換を許可または受諾してはなりません。 コントロールには、鍵コンポーネントまたは鍵共有にアクセスできる個人が、鍵を導出するために必要な閾値を形成する他の鍵コンポーネントまたは鍵共有へのアクセス権を付与しないことが含まれる必要があります。
カスタマイズアプローチの目的		
暗号化鍵は、権限のない担当者が交換することはできない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** このプロセスは、鍵管理者として活動する個人が、鍵管理者の役割にコミットし、その責任を理解し、受諾することを保証するのに有用です。年 1 回の再確認は、鍵管理者の責任を再認識させるのに役立ちます。 **その他の情報** 鍵管理者およびその役割と責任に関する業界ガイダンスには、以下のものがあります。 • *NIST SP 800-130 暗号鍵管理システム設計のためのフレームワーク*[5.鍵管理者の役割と責任（特に）]。 • *ISO 11568-1 バンキング– 鍵管理（リテール）-- パート 1*:原則 [鍵管理の 5 原則(特に b)] について
3.7.8 鍵管理のポリシーおよび手順が、暗号化鍵の管理者が鍵の管理者としての責任を理解し受け入れ、（書面または電子的に）正式に承認することを含めて実施されている。	**3.7.8.a** 保存されているアカウントデータの保護に使用される鍵の文書化された鍵管理ポリシーおよび手順を調査し、この要件で指定されているすべての要素に従って、鍵管理者の確認事項を定義していることを確認する。	
	3.7.8.b 鍵管理者がこの要件で指定されたすべての要素に従って確認書を提供したことを示す文書または他の証拠を確認する。	
カスタマイズアプローチの目的 鍵管理者は、暗号運用に関連する責任について知識があり、必要なときに支援やガイダンスにアクセスすることができる。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 暗号鍵の安全な伝送、保存、更新の方法について顧客にガイダンスを提供することは、鍵の管理上のミスや無許可の事業体への漏洩の防止に役立ちます。 **その他の情報** 鍵管理に関する多くの業界標準は、上記の要件 3.7.1～3.7.8 のガイダンスに引用されています。
3.7.9 ***サービスプロバイダのみに対する追加要件：*** サービスプロバイダが、アカウントデータの伝送または保存のために、その顧客と暗号鍵を共有する場合、当該鍵の安全な伝送、保存、更新に関するガイダンスが文書化され、サービスプロバイダの顧客に配布される。 *(次ページに続く)*	**3.7.9** ***サービスプロバイダ評価のみの追加テスト手順：*** サービスプロバイダがアカウントデータの伝送または保存のために暗号鍵を顧客と共有する場合、サービスプロバイダが顧客に提供する文書を調査し、上記の要件 3.7.1 から 3.7.8 に規定されるすべての要素に従って顧客の鍵を安全に伝送、保存、更新する方法に関する指針が含まれていることを確認する。	

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 顧客は、共有される暗号鍵を受け取るたびに、適切な鍵管理のガイダンスを提供される。 **適用に関する注意事項** この要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用される。		

要件 4：　オープンな公共ネットワークでの送信時に、強力な暗号化技術でカード会員データを保護する

セクション	
4.1	オープンな公共ネットワークを介した伝送中に、強力な暗号化技術を使用してカード会員データを保護するためのプロセスおよびメカニズムが定義され、文書化されていること。
4.2	PAN は、送信時に強力な暗号で保護される

概要

強力な暗号化技術の使用により、データの機密性、完全性、および非否認性をより確実に保持することができる。

漏洩から保護するためには、信頼されていないネットワークや公衆ネットワークなど、悪意のある個人が容易にアクセスできるネットワークを介して PAN を送信する際に暗号化する必要がある。無線ネットワークの設定の誤りや、従来の暗号化および認証プロトコルの脆弱性は、カード会員データ環境（CDE）への特権的アクセスを目的として、これらの脆弱性を悪用しようとする悪意のある人物に狙われ続けている。カード会員データを保存、処理、または伝送するネットワークがあるため、企業の内部ネットワークでカード会員データを伝送すると、そのネットワークは当然ながら PCI DSS の適用範囲に含まれる。そのようなネットワークは、適用される PCI DSS 要件に対して評価および査定される必要がある。

要件 4 は、個別の要件で特に指定されていない限り、PAN の伝送に適用される。

PAN 送信は、送信前のデータの暗号化、またはデータが送信されるセッションの暗号化、もしくはその両方によって保護することができる。データレベルとセッションレベルの両方で強力な暗号化技術を適用することは必須ではないが、推奨される。

「強力な暗号化技術」およびその他の PCI DSS 用語の定義については、付録 G を参照すること。

要件とテスト手順		ガイダンス
4.1 オープンな公共ネットワークを介した伝送中に、強力な暗号化技術でカード会員データを保護するための プロセスおよびメカニズムが定義され、文書化されている。		
定義されたアプローチの要件 **4.1.1** 要件 4 で特定されたすべてのセキュリティポリシーと運用手順が • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • 影響を受ける関係者全員に知らされている。 **カスタマイズアプローチの目的** 要件 4 内の活動を満たすための期待、コントロール、および監視が定義され、影響を受ける担当者によって順守されている。すべての支援活動が繰り返し可能であり、一貫して適用され、経営者の意図に適合している。	**定義されたアプローチのテスト手順** **4.1.1** 要件 4 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューを行う。	**目的** 要件 4.1.1 は、要件 4 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 4 に関連する特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及することを保証することも同様に重要です。 **グッドプラクティス** プロセス、技術、ビジネス目的の変化に対応するため、必要に応じてポリシーと手順を更新することが重要です。そのため、定期的な更新だけでなく、変更があった場合はできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、企業のセキュリティの目的および原則を定義するものです。運用手順は、活動の実行方法を記述し、一貫した方法で、ポリシーの目的に従って望ましい結果を達成するために従う統制、方法、プロセスを定義します。ポリシーおよび手順は、更新を含め、影響を受けるすべての担当者に積極的に伝達され、活動の実行方法を記述した運用手順によって支援されています。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要な活動が行われない可能性があります。 **グッドプラクティス** 役割と責任は、ポリシーと手順の中で文書化されるか、または別の文書で管理されるかもしれません。 役割と責任を伝える一環として、事業体は担当者に与えられた役割と責任を受け入れ、理解することを認めさせることを検討することができます。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担表（RACI マトリクスとも呼ばれる）があります。
4.1.2 要件 4 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**4.1.2.a** 文書を調査し、要件 4 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	4.1.2.b 要件 4 の活動の実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 4 のすべての活動を実施するための日常的な責任が割り当てられている。担当者は、これらの要件の成功裏に、継続的に運用する責任を負う。		

要件とテスト手順		ガイダンス
4.2 送信時の PAN は強力な暗号化技術で保護されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
4.2.1 強力な暗号とセキュリティプロトコルを以下のように実装し、オープンな公共ネットワークでの送信時に PAN を保護する。 • 信頼できる鍵および証明書のみを受け付ける。 • オープンな公共ネットワークを介した送信時に PAN を保護するために使用される証明書は、有効であることが確認され、有効期限が切れていたり失効していないこと。*この箇条は発効日までのベストプラクティスであり、詳細は以下の適用上の注意を参照すること。* • 使用中のプロトコルは安全なバージョンや設定のみをサポートし、安全でないバージョン、アルゴリズム、鍵サイズ、実装へのフォールバックや使用はサポートしない。 • 暗号強度は使用中の暗号化方式に適したものである。	**4.2.1.a** 文書化されたポリシーと手順を調べ、担当者にインタビューして、この要件で指定されているすべての要素を含むようにプロセスが定義されていることを確認する。	機密性の高い情報は、公衆ネットワーク上で送信される際に暗号化されなければなりません。なぜなら、悪意のある個人が送信中のデータを傍受したり転用したりすることは簡単で一般的なことだからです。
	4.2.1.b システム構成を調査し、この要件で指定されたすべての要素に従って強力な暗号化およびセキュリティプロトコルが実装されていることを確認する。	**グッドプラクティス** 要件 1 で定義されたデータフロー図とネットワーク図は、オープンな公共ネットワーク上でアカウントデータが送受信されるすべての接続ポイントを特定するための有用なリソースです。 必須ではありませんが、事業体は内部ネットワーク上の PAN も暗号化し、新しいネットワーク実装では暗号化通信を確立することが望ましいと考えられます。 PAN 送信は、送信前のデータの暗号化、またはデータが送信されるセッションの暗号化、もしくはその両方によって保護することができます。データレベルとセッションレベルの両方で強力な暗号化技術を適用することは必須ではありませんが、強く推奨します。データレベルで暗号化する場合、データ保護に使用する暗号鍵は要件 3.6 および 3.7 *(次ページに続く)*
	4.2.1.c カード会員データの送信を調査し、すべての PAN がオープンな公共ネットワークで送信される場合、強力な暗号化技術で暗号化されていることを確認する。	
	4.2.1.d システム構成を調査し、信頼できることが確認できない鍵および／または証明書が拒否されることを確認する。	
カスタマイズアプローチの目的		
オープンな公共ネットワークを介した通信では、平文の PAN を読み取ったり、傍受したりすることはできない。		

要件とテスト手順		ガイダンス
適用に関する注意事項		に従って管理することが可能です。データがセッションレベルで暗号化されている場合、指定された鍵管理者が送信鍵および証明書の管理責任を負うべきです。 一部のプロトコル実装（SSL、SSH v1.0、初期の TLS など）には、攻撃者が平文データにアクセスするために使用できる既知の脆弱性があります。事業体は、使用している暗号スイートについて業界で決められた廃止日を常に認識し、古いものが安全でないと判断された場合に新しいバージョンまたはプロトコルに移行できるよう準備しておくことが重要です。 証明書が信頼できるものであることを確認することは、安全な接続の完全性を保証するのに役立ちます。信頼できる証明書とは、信頼できる認証局（CA）のような信頼できるソースから発行され、有効期限が切れていないものです。証明書の検証には、最新の証明書失効リスト（CRL）またはオンライン証明書状態プロトコル（OCSP）を使用することができます。 証明書を検証する技術には、信頼できる証明書または公開鍵を開発中または最初の使用時に固定する、証明書や公開鍵ピニング（PKP）が含まれる場合があります。 *(次ページに続く)*
事業体が、機密データの受信を意図していない安全でない通信チャネルを介して、カード会員データを未承認で受信する場合がある。この場合、事業体は、カード会員データ環境（CDE） の範囲にチャネルを含めて PCI DSS に従って保護するか、チャネルがカード会員データに使用されるのを防止するための手段を講じるかを選択できる。 自己署名入り証明書は、証明書が組織内の CA によって発行され、証明書の作成者が確認され、証明書がハッシュまたは署名などの方法で検証され、有効期限が切れていない場合に受け入れられる可能性がある。ただし、「発行元」と「発行先」の識別名（DN）フィールドが同じである自己署名証明書は認められない。 *上記の項目（オープンな公共ネットワークを介した送信時に PAN を保護するために使用される証明書が有効であり、有効期限が切れていない、または失効していないことの確認）は、2025 年 3 月 31 日までのベストプラクティスであり、それ以降は要件 4.2.1 の一部として要件となり、PCI DSS 評価中に十分に考慮する必要がある。*		

要件とテスト手順		ガイダンス
		また、開発者に確認したり、ソースコードをレビューしたりして、証明書が不良の場合にクライアントやサーバが接続を拒否するようにすることもできます。 ブラウザベースの TLS 証明書では、アドレスバーの横に表示される鍵のアイコンをクリックすることで、証明書の信頼性を確認できることがよくあります。 **例** オープンな公共ネットワークには、以下のものが含まれますが、これらに限定されるものではありません。 • インターネットおよび • Wi-Fi、Bluetooth、セルラー技術、衛星通信などの無線技術 *(次ページに続く)*

要件とテスト手順		ガイダンス
		その他の情報 使用する暗号化方式に応じた適切な暗号強度の情報については、ベンダの推奨事項や業界のベストプラクティスを参照することができます。 強力な暗号化技術と安全なプロトコルの詳細については、*NIST SP 800-52* および *SP 800-57* などの業界標準とベストプラクティスを参照してください。 信頼できる鍵や証明書の詳細については、以下を参照してください。*NIST サイバーセキュリティ実践ガイド特別刊行物 1800-16「ウェブトランザクションの保護」、トランスポート・レイヤー・セキュリティ（TLS）サーバ証明書管理*

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 信頼できる鍵のインベントリは、事業体がアルゴリズム、プロトコル、鍵の強度、鍵の保管者、鍵の有効期限を追跡するのに役立つ。これにより、事業体は、暗号化ソフトウェア、証明書、および暗号アルゴリズムに発見された脆弱性 に迅速に対応することができる。 **グッドプラクティス** 証明書については、インベントリには、発行認証機関および証明書の有効期限を含めるものとする。
4.2.1.1 送信中の PAN を保護するために使用される事業体の_信頼できる鍵および証明書のインベントリが維持されている。	**4.2.1.1.a** 文書化されたポリシーおよび手順を調査し、事業体が信頼できる鍵および証明書のインベントリを維持するためのプロセスが定義されていることを検証する。	
	4.2.1.1.b 信頼できる鍵および証明書のインベントリを調べ、それが最新の状態に維持されていることを検証する。	
カスタマイズアプローチの目的		
送信中の PAN を保護するために使用されるすべての鍵と証明書が識別され、信頼されていることが確認され る。		
適用上の注意		
この要件は 2025 年 3 月 31 日まではベストプラクティスですが、それ以降は必須となるため、PCI DSS 評価中に十分に検討する必要があります。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 無線ネットワークは接続に物理的な媒体を必要としないため、誰が接続できるか、どのような伝送プロトコルを使用するかを制限する制御を確立することが重要です。悪意のあるユーザは、無線通信を盗聴するために無料で広く利用可能なツールを使用します。強力な暗号を使用することで、ワイヤレスネットワーク上での機密情報の漏洩を制限することができます。 ワイヤレス・ネットワークは、事業体に固有のリスクをもたらすため、業界の要件に従って識別し、保護する必要があります。悪意のあるユーザがワイヤレスネットワークにアクセスしたり、ワイヤレスネットワークを利用して他の内部ネットワークやデータにアクセスしたりすることを防ぐには、強力な暗号化が認証と PAN の送信に必要です。 **グッドプラクティス** 無線ネットワークは、強力な暗号の意図を満たさない安全でないプロトコルや低い暗号強度へのフォールバックやダウングレードを許可してはなりません。 **その他の情報** 暗号に関連するプロトコルの選択、構成、設定の詳細については、各ベンダのドキュメントを参照すること。
4.2.1.2 PAN を送信する、またはカード会員データ環境（CDE）に接続するワイヤレスネットワークは、認証と送信に強力な暗号を実装するために業界のベストプラクティスを使用する。	**4.2.1.2** システム構成を調べ、PAN を送信する、またはカード会員データ環境（CDE）に接続する無線ネットワークが、認証と送信に強力な暗号を実装する業界のベストプラクティスを使用していることを確認する。	
カスタマイズアプローチの目的		
無線ネットワーク通信から、クリアテキストの PAN を読み取ったり、傍受したりすることはできない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
4.2.2 エンドユーザメッセージングテクノロジを介して送信される場合、PAN は常に強力な暗号で保護される。	**4.2.2.a** 文書化されたポリシーと手順を調べ、エンドユーザメッセージングテクノロジで送信されるときは常に、強力な暗号で PAN を保護するためのプロセスが定義されていることを確認する。	**目的** エンドユーザのメッセージングテクノロジは、通常、内部ネットワークや公共ネットワークでの配信中にパケットスニッフィングによって簡単に傍受される可能性があります。 **グッドプラクティス** エンドユーザメッセージングテクノロジを使用して PAN を送信することは、明確なビジネスニーズがある場合にのみ検討する必要があります。 **例** 電子メール、インスタントメッセージ、SMS、チャットは、この要件が言及するタイプのエンドユーザメッセージングテクノロジの例です。
カスタマイズアプローチの目的 エンドユーザメッセージングテクノロジを使用した送信から、クリアテキストの PAN を読み取ったり、傍受したりすることはできない。	**4.2.2.b** システム構成とベンダの文書を調査し、エンドユーザメッセージングテクノロジを介して送信されるときは常に、PAN が強力な暗号で保護されていることを確認する。	
適用上の注意 この要件は、顧客またはその他のサードパーティが、エンドユーザメッセージングテクノロジを使用して PAN を送信するよう要求した場合にも適用される。 事業体が、機密データの送信を意図していない安全でない通信チャネルを介して、未承諾のカード会員データを受信する場合もあり得ます。この場合、事業体は、カード会員データ環境（CDE） の範囲にチャネルを含めて PCI DSS に従って保護するか、カード会員データを削除してチャネルがカード会員データに使用されるのを防止するための措置を講じるかを選択できる。		

脆弱性管理プログラムの維持

要件 5：　悪意のあるソフトウェアからすべてのシステムおよびネットワークを保護する

セクション	
5.1	すべてのシステムおよびネットワークを悪意あるソフトウェアから保護するためのプロセスおよびメカニズムが定義され、理解されている。
5.2	悪意のあるソフトウェア（マルウェア）が防止されている、または検知され対処されている。
5.3	マルウェア対策の仕組みとプロセスが有効であり、維持され、監視されている。
5.4	フィッシング対策の仕組みで、フィッシング攻撃からユーザを保護する。

概要

悪意のあるソフトウェア（マルウェア）とは、所有者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、可用性を損なう目的で、所有者の認識または同意なしにコンピュータシステムに侵入または損傷を与えるように設計されたソフトウェアまたはファームウェアのことです。

ウイルス、ワーム、トロイの木馬、スパイウェア、ランサムウェア、キーロガー、ルートキット、悪意のあるコード、スクリプト、リンクなどがその例です。

マルウェアは、従業員の電子メール（フィッシングなど）やインターネット、モバイルコンピューター、ストレージデバイスの使用など、業務上認められている多くの活動中にネットワークに侵入し、システムの脆弱性を突く結果となることがあります。

あらゆる種類のマルウェアに対応するマルウェア対策ソリューションを使用することで、現在進行形で進化するマルウェアの脅威からシステムを保護することができます。

PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
5.1 全てのシステムおよびネットワークを悪意のあるソフトウェアから保護するためのプロセスおよびメカニズムが定義され、理解されている。		
定義されたアプローチの要件 **5.1.1** 要件 5 で特定されたすべてのセキュリティポリシーと運用手順が • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に知られている。 **カスタマイズアプローチの目的** 要件 5 内の活動を満たすための期待、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべての支援活動が繰り返し一貫して適用可能であり、経営者の意図に適合している。	**定義されたアプローチのテスト手順** **5.1.1** 要件 5 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューを行う。	**目的** 要件 5.1.1 は、要件 5 を通して指定された様々なポリシーと手順を効果的に管理し、維持することに関するものです。要件 5 で呼び出された特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及していることを確認することも同様に重要です。 **グッドプラクティス** プロセス、技術、ビジネス目的の変化に対応するため、必要に応じてポリシーと手順を更新することが重要です。そのため、定期的な更新だけでなく、変更があった場合はできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、企業のセキュリティの目的および原則を定義するものです。運用手順は、活動の実行方法を記述し、一貫した方法で、ポリシーの目的に従って望ましい結果を達成するために従う統制、方法、プロセスを定義します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
5.1.2 要件 5 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**5.1.2.a** 文書を調査し、要件 5 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	役割と責任が正式に割り当てられていない場合、ネットワークやシステムがマルウェアから適切に保護されない可能性があります。 **グッドプラクティス** 役割と責任は、方針と手順の中で文書化されるか、または別の文書で管理されることができます。 役割と責任を伝える一環として、事業体は、担当者に与えられた役割と責任を受け入れ、理解することを認めさせることを検討することができます。 **例** 役割と責任を文書化する方法として、責任者、説明責任者、相談役、情報提供者を含む責任分担マトリックス（RACI マトリックスとも呼ばれる）があります。
	5.1.2.b 要件 5 の活動の実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 5 のすべての活動を実施するための日常的な責任が割り当てられている。担当者は、これらの要件の成功、継続的な運用に責任を負う。		

要件とテスト手順		ガイダンス
5.2 悪意のあるソフトウェア（マルウェア）が防止または検出され、対処されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** これまで安全とされてきたシステムにおいて、新たに発見された脆弱性を狙った攻撃が後を絶ちません。定期的に更新されるマルウェア対策ソリューションがなければ、新しい形態のマルウェアがシステム攻撃、ネットワークの無効化、データの漏洩に利用される可能性があります。 **グッドプラクティス** ゼロデイ攻撃（未知の脆弱性を悪用した攻撃）を意識し、行動特性に着目し、予期せぬ行動に対して警告・反応するソリューションを検討することが有益です。 **定義** マルウェアの影響を受けることが知られているシステム・コンポーネントは、現実世界で利用可能なアクティブなマルウェアのエクスプロイト（理論上のエクスプロイトだけでなく）を持っています。
5.2.1 要件 5.2.3 による定期的な評価で、マルウェアによるリスクがないと判断されたシステムコンポーネントを除く、すべてのシステムコンポーネントにマルウェア対策ソリューションが配備されていること。	**5.2.1.a** システムコンポーネントを調査し、要件 5.2.3 に基づく定期的な評価によりマルウェアのリスクがないと判断されたコンポーネントを除く、すべてのシステムコンポーネントにマルウェア対策ソリューションが導入されていることを確認する。 **5.2.1.b** マルウェア対策ソリューションがないシステムコンポー ネントについては、定期的な評価を調べ、そのコンポーネントが評価され、マルウェアのリスクがないとの結論が出されていることを確認する。	
カスタマイズアプローチの目的 システムがマルウェアの攻撃ベクトルとなることを防ぐために、自動化されたメカニズムが導入されている。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 不正なアクセスを防ぐためには、あらゆる種類のマルウェアから保護することが重要です。 **グッドプラクティス** マルウェア対策ソリューションには、ネットワークベースの制御、ホストベースの制御、およびエンドポイントセキュリティソリューションの組み合わせが含まれる場合があります。最近のマルウェア対策ソリューションでは、シグネチャベースのツールに加え、サンドボックス、権限昇格の制御、機械学習などの機能が使用されています。 ソリューションの技術には、マルウェアがネットワークに侵入するのを防ぐこと、ネットワークに侵入したマルウェアを除去または封じ込めることが含まれます。 **例** マルウェアには、ウイルス、トロイの木馬、ワーム、スパイウェア、ランサムウェア、キーロガー、ルートキット、悪意のあるコード、スクリプト、リンクなどが含まれますが、これらに限定されるものではありません。
5.2.2 導入されたマルウェア対策ソリューションは以下の通りであること。 • 既知のすべての種類のマルウェアを検出する。 • 既知のマルウェアの種類をすべて削除、ブロック、または封じ込める。	**5.2.2** マルウェア対策ソリューションのベンダの文書および設定を調査し、そのソリューションが以下のとおりであることを確認する。 • 既知のすべての種類のマルウェアを検出する。 • 既知のマルウェアの種類をすべて削除、ブロック、または封じ込める。	
カスタイマイズアプローチの目的		
マルウェアが他のシステムコンポーネントを実行したり感染したりできないようにする。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
5.2.3 マルウェアのリスクがないシステムコンポーネントは定期的に評価され、以下の内容が含まれる。 • マルウェアのリスクがないすべてのシステムコンポーネントの文書化されたリスト。 • これらのシステムコンポーネントについて、進化するマルウェアの脅威を特定し、評価する。 • そのようなシステムコンポーネントが引き続きマルウェア対策の保護を必要としないかどうかの確認。	**5.2.3.a** 文書化されたポリシーと手順を調べ、マルウェアのリスクがないシステムコンポーネントの定期的な評価のために、この要件で指定されたすべての要素を含むプロセスが定義されていることを確認する。	ある時点では、特定のシステムがマルウェアの標的となったり、影響を受けたりすることはあまりないかもしれません。例えば、ベンダのセキュリティ通知やマルウェア対策フォーラムを監視し、自社のシステムが新しいマルウェアの脅威にさらされているかどうかを判断することが重要です。
カスタイマイズアプローチの目的	**5.2.3.b** 評価にはこの要件で指定されたすべての要素が含まれていることを確認するために、担当者にインタビューを行う。	**グッドプラクティス**
マルウェアから保護されていないシステムが感染のリスクにさらされないように、事業体は進化するマルウェアの脅威に対する認識を維持する。	**5.2.3.c** マルウェアのリスクがないと特定されたシステムコンポーネントのリストを調べ、要件 5.2.1 に従ってマルウェア対策ソリューションを導入していないシステムコンポーネントと比較し、システムコンポーネントが両方の要件に一致することを確認する。	企業が特定のシステムがマルウェアの影響を受けないと判断する場合、その判断は業界の証拠、ベンダのリソース、ベストプラクティスによって裏付けられる必要があります。 定期的な評価には、以下の手順が有効です。 • 過去にマルウェア対策が不要と判定されたシステムの種類をすべて特定する。 • 業界の脆弱性アラートおよび通知を確認し、特定したシステムに新たな脅威が存在するかどうかを判断する。 • マルウェアの影響を受けないシステムであるかどうかの結論を文書化する。 *(次ページに続く)*
適用上の注意		
この要件の対象となるシステムコンポーネントは、要件 5.2.1 に従ってマルウェア対策ソリューションが配備されていないものである。		

要件とテスト手順		ガイダンス
		• マルウェア対策が必要となったシステムタイプに対して、マルウェア対策を追加する戦略。 マルウェアの傾向は、要件 6.3.1 における新しいセキュリティ脆弱性の特定に含め、新しい傾向に対処する方法を、必要に応じて事業体の構成基準および保護メカニズムに組み込む必要があります。
定義されたアプローチの要件 **5.2.3.1** マルウェアのリスクがないと特定されたシステムコンポーネントの定期的な評価の頻度は、事業体のターゲットリスク分析で定義され、要件 12.3.1 で指定されたすべての要素に従って実行される。	**定義されたアプローチのテスト手順** **5.2.3.1.a** マルウェアのリスクがないと識別されたシステムコンポーネントの定期的な評価の頻度について、事業体のターゲットリスク分析を調べ、リスク分析が要件 12.3.1 に規定されるすべての要素に従って実施されたことを確認する。	**目的** 事業者は、各事業者の環境の複雑さ、評価が必要なシステムの種類数などの基準に基づいて、最適な評価実施期間を決定します。
カスタイマイズアプローチの目的 マルウェアのリスクにさらされていないシステムは、事業者のリスクに対応した頻度で再評価される。	**5.2.3.1.b** マルウェアのリスクがないと識別されたシステムコンポーネントの定期的な評価の文書化された結果を調べ、この要件のために実施された事業体のターゲットリスク分析で定義された頻度で評価が実施されていることを検証するために担当者にインタビューする。	
適用上の注意 この要件は 2025 年 3 月 31 日まではベストプラクティスであるが、それ以降は必須となるため、PCI DSS 評価中に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
5.3 マルウェア対策メカニズムおよびプロセスがアクティブであり、維持され、監視されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** マルウェア対策ソリューションの効果を維持するためには、最新のセキュリティアップデート、シグネチャ、脅威分析エンジン、およびソリューションが依存するその他のマルウェア保護機能を備えている必要があります。 自動化された更新プロセスにより、エンドユーザが手動で更新プログラムをインストールする負担を回避し、更新プログラムがリリースされた後、マルウェア対策メカニズムができるだけ早く更新されることをより確実にすることができます。 **グッドプラクティス** マルウェア対策は、更新プログラムが利用可能になった後、できるだけ早く信頼できるソース経由で更新する必要があります。信頼できる共通のソースを使用してエンドユーザシステムにアップデートを配布することで、ソリューションアーキテクチャの整合性と一貫性を確保することができます。 アップデートは、個々のシステム・コンポーネントに展開される前に、例えばテストを可能にするために、自動的に中央ロケーションにダウンロードされることがあります。
5.3.1 マルウェア対策ソリューションが自動更新により最新の状態に保たれている。	**5.3.1.a** ソフトウェアのマスターインストールを含むマルウェア対策ソリューションの構成を調査し、自動更新を実行するように構成されていることを確認する。	
	5.3.1.b システムコンポーネントとログを調査し、マルウェア対策ソリューションと定義が最新であり、迅速に展開されていることを確認する。	
カスタイマイズアプローチの目的		
マルウェア対策機構が、最新のマルウェアの脅威を検知し、対処できること。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
5.3.2 マルウェア対策ソリューションは以下を満たすこと。 • 定期的なスキャンとアクティブスキャンまたはリアルタイムスキャンを実行する。 **または** • システムまたはプロセスの継続的な振る舞い分析を行う。	**5.3.2.a** ソフトウェアのマスターインストールを含むマルウェア対策ソリューションの構成を調べ、この要件で指定された要素の少なくとも 1 つを実行するようにソリューションが構成されていることを確認する。	定期的なスキャンにより、環境内に存在するが、現在は活動していないマルウェアを特定することができる。ゼロデイマルウェアのように、スキャンソリューションが検出する前に環境内に侵入するマルウェアもあります。定期的なスキャンやシステムまたはプロセスの継続的な振る舞い分析を行うことで、以前は検出できなかったマルウェアを確実に特定、除去し、環境へのアクセス経路を特定するために調査することができます。
	5.3.2.b マルウェアのリスクがあると特定されたすべてのオペレーティングシステムの種類を含むシステムコンポー ネントを調べ、この要件で指定された要素の少なくとも 1 つに従ってソリューションが有効であることを確認す る。	**グッドプラクティス** 定期的なスキャン（スケジュールおよびオンデマンド）とアクティブなリアルタイムスキャン（オンアクセス）を組み合わせて使用することにより、カード会員データ環境（CDE）の静的および動的要素に存在するマルウェアに確実に対処することができます。また、疑わしい活動が検出された場合、ユーザは自分のシステム上でオンデマンドスキャンを実行できるようにする必要があり、これはマルウェアの早期発見に役立ちます。
カスタイマイズアプローチの目的	**5.3.2.c** ログとスキャン結果を調査し、この要件で指定された要素の少なくとも 1 つに従ってソリューションが有効であることを確認する。	*(次ページに続く)*
マルウェアが実行を完了できない。		

要件とテスト手順		ガイダンス
		スキャンは、すべてのディスク、メモリ、起動ファイル、ブートレコード（システム再起動時）を含むファイルシステム全体を対象とし、システム上に常駐しているが現在はアクティブではないソフトウェアも含め、ファイル実行時にすべてのマルウェアを検出する必要があります。スキャン範囲は、電子メールサーバ、ウェブブラウザ、インスタントメッセージングソフトウェアなど、見落とされがちなものを含むカード会員データ環境（CDE）内のすべてのシステムおよびソフトウェアを含むべきです。 **定義** アクティブスキャン（リアルタイムスキャン）は、ファイルを開く、閉じる、名前を変更するなどの操作を行った際にマルウェアの有無をチェックし、マルウェアが起動するのを防ぎます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
5.3.2.1 要件 5.3.2 を満たすために定期的なマルウェアスキャンを実施する場合、スキャンの頻度は、要件 12.3.1 に規定されるすべての要素に従って実施される事業体のターゲットリスク分析において定義される。	**5.3.2.1.a** 定期的なマルウェアスキャンの頻度に関する事業体のターゲットリスク分析を調べ、リスク分析が要件 12.3.1 で指定されたすべての要素に従って実施されたことを確認する。 **5.3.2.1.b** 定期的なマルウェアスキャンの文書化された結果を調査し、担当者にインタビューして、この要件のために実施した事業体のターゲットリスク分析で定義された頻度でスキャンが実行されていることを確認する。	定期的なスキャンを実施する最適な期間は、各自の環境にもたらされるリスクの評価に基づいて決定することができます。
カスタイマイズアプローチの目的		
マルウェアソリューションによるスキャンが、事業者のリスクに対応した頻度で実施されている。		
適用上の注意		
この要件は、要件 5.3.2 を満たすために定期的なマルウェアスキャンを実施する事業者に適用される。 この要件は 2025 年 3 月 31 日まではベストプラクティスであるが、それ以降は必須となるため、PCI DSS 評価中に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
5.3.3 リムーバブル電子メディアの場合、マルウェア対策のソリューションは以下を満たすこと： • メディアが挿入、接続、または論理的にマウントされたときに自動スキャンを実行する。 **または** • メディアが挿入、接続、または論理的にマウントされているときに、システムまたはプロセスの継続的な振る舞い分析を実行する。	**5.3.3.a** マルウェア対策ソリューションの構成を調査し、取り外し可能な電子メディアについて、この要件で指定された要素の少なくとも 1 つを実行するように構成されていることを確認する。 **5.3.3.b** リムーバブル電子メディアが接続されたシステムコンポーネントを調べ、この要件で規定されている要素の少なくとも 1 つに従ってソリューション（複数可）が有効になっていることを確認する。 **5.3.3.c** ログとスキャン結果を調査し、この要件で指定された要素の少なくとも 1 つに従ってソリューションが有効であることを確認する。	ポータブルメディアデバイスは、マルウェアの侵入経路として見過ごされがちです。攻撃者はしばしば、USB やフラッシュドライブなどのポータブルデバイスにマルウェアを事前にロードし、感染したデバイスをコンピュータに接続するとマルウェアが起動し、環境内に新たな脅威をもたらすことになります。
カスタイマイズアプローチの目的		
外部リムーバブルメディア経由でシステムコンポーネントにマルウェアを持ち込むことができない。		
適用上の注意		
この要件は 2025 年 3 月 31 日まではベストプラクティスであるが、それ以降は必須となるため、PCI DSS 評価中に十分に検討する必要がある。		
(次ページに続く)		

<table>
<tr><th colspan="2">要件とテスト手順</th><th>ガイダンス</th></tr>
<tr><td>定義されたアプローチの要件</td><td>定義されたアプローチのテスト手順</td><td rowspan="2">目的
例えば、アップデートやスキャンが期待通りに実行されているか、マルウェアが特定され対処されているかを確認することで、マルウェア対策メカニズムの有効性を追跡することが重要です。また、監査ログにより、マルウェアがどのように環境に侵入したかを判断し、企業のネットワーク内部におけるその活動を追跡することができます。</td></tr>
<tr><td>5.3.4 マルウェア対策ソリューションの設定を調査し、要件 10.5.1 に従ってログが有効化され保持されていることを確認する。</td><td>5.3.4 マルウェア対策ソリューションの構成を調査し、要件 10.5.1 に従ってログが有効化され保持されていることを確認する。</td></tr>
<tr><td>カスタイマイズアプローチの目的</td><td rowspan="2"></td></tr>
<tr><td>マルウェア対策活動の履歴記録がすぐに利用でき、少なくとも 12 カ月間保持される。</td></tr>
<tr><td>定義されたアプローチの要件</td><td>定義されたアプローチのテスト手順</td><td rowspan="3">目的
マルウェアをリアルタイムに検知するためには、防御機構が常に稼働していることが重要です。マルウェア対策ソリューションをアドホックに起動・停止すると、マルウェアがチェックされず、検出されずに増殖する可能性があります。

(次ページに続く)</td></tr>
<tr><td>5.3.5 マルウェア対策機構は、特に文書化され、管理者が限定期間内にケースバイケースで許可しない限り、ユーザが無効にしたり変更したりすることはできない。</td><td>5.3.5.a マルウェア対策の構成を調査し、マルウェア対策機構がユーザによって無効化または変更できないことを確認する。</td></tr>
<tr><td>カスタイマイズアプローチの目的</td><td rowspan="2">5.3.5.b 担当者にインタビューを行い、プロセスを観察し、マルウェア対策機構を無効化または変更する要求が具体的に文書化され、期間限定で管理</td></tr>
<tr><td>マルウェア対策機構は、権限のない担当者が変更することはできない。</td></tr>
</table>

要件とテスト手順		ガイダンス
適用上の注意 マルウェア対策ソリューションは、ケースバイケースで管理者が許可する正当な技術的必要性がある場合にのみ、一時的に無効化することができる。特定の目的のためにマルウェア対策を無効にする必要がある場合は、正式に承認されなければならない。また、マルウェア対策が有効でない期間については、追加のセキュリティ対策を実施する必要がある場合がある。	者によってケースバイケースで承認されていることを確認する。	**グッドプラクティス** 特定の保守作業や技術的な問題の調査をサポートするために、システムのマルウェア対策を一時的に無効にする正当な必要性がある場合、そのような措置を取る理由を理解し、適切な管理責任者の承認を受ける必要があります。管理者自身のデバイスを含め、マルウェア対策機構の無効化または変更は、権限を与えられた担当者によって実行されるべきである。管理者が自分のコンピュータのマルウェア対策を無効にできる権限を持っていることは認識されていますが、そのようなソフトウェアが無効にされたときに警告する仕組みがあり、その後、正しいプロセスに従ったことを確認するためのフォローアップが行われる必要があります。 **例** マルウェア対策が有効でない期間に実施する必要がある追加のセキュリティ対策としては、マルウェア対策が無効になっている間は保護されていないシステムをインターネットから切り離し、再度有効になった時点で完全スキャンを実行することなどが挙げられます。

要件とテスト手順		ガイダンス
5.4 フィッシング対策機構は、フィッシング攻撃からユーザを保護する。		
定義されたアプローチの要件 **5.4.1** フィッシング攻撃を検知し、担当者を保護するためのプロセスや自動化されたメカニズムがある。 **カスタイマイズアプローチの目的** フィッシング攻撃から保護し、リスクを軽減するための仕組みがある。 **適用上の注意** この要件は、自動化されたメカニズムに適用される。このような自動化されたメカニズムを提供するシステムおよびサービス（電子メールサーバなど）を PCI DSS の適用範囲に入れることは意図していない。 この要件の焦点は、PCI DSS の適用範囲にあるシステム構成要素にアクセスする担当者を保護することである。 フィッシングを検出して作業員を保護するための技術的および自動的なコントロールに関するこの要件を満たすことは、セキュリティ意識向上トレーニングに関する要件 12.6.3.1 と同じではない。 *(次ページに続く)*	**定義されたアプローチのテスト手順** **5.4.1** フィッシング攻撃を検知し、従業員を保護するための管理体制が整っていることを確認するために、実施されたプロセスを観察し、仕組みを検証する。	**目的** 技術的なコントロールにより、担当者がコミュニケーションの真偽を評価する機会を制限することができ、また、フィッシングに対する個々の対応の影響を制限することができます。 **グッドプラクティス** フィッシング対策を行う際には、複数のアプローチを組み合わせて検討することが推奨されます。例えば、DMARC（Domain-based Message Authentication, Reporting & Conformance）、センダーポリシーフレームワーク（SPF）、ドメインキー識別メール（DKIM）などのスプーフィング対策は、フィッシャーが企業のドメインを詐称し、社員になりすますのを阻止するのに効果的です。 リンク・スクラバーやサーバサイドのマルウェア対策など、フィッシングメールやマルウェアが担当者に届く前にブロックする技術を導入することで、インシデントを減らし、担当者がフィッシング攻撃をチェックし報告するのに要する時間を短縮することができます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
この要件を満たすことは、担当者にセキュリティ意識向上トレーニングを提供するための要件を満たすことでもなく、その逆も同様である。 *この要件は 2025 年 3 月 31 日まではベストプラクティスであるが、それ以降は必須となるため、PCI DSS 評価中に十分に検討する必要がある。*		さらに、フィッシング・メールを認識し報告するよう担当者を訓練することで、類似したメールを識別し、開封する前に削除することができるようになります。 フィッシング対策は、企業の事業体全体に適用されることが推奨されます（必須ではありません）。 **定義** フィッシングとは、ソーシャルエンジニアリングの一種で、攻撃者がユーザアカウント名やパスワード、アカウントデータなどの機密情報を開示させるために用いるさまざまな方法を指します。攻撃者は通常、自身を偽装し、本物または信頼できる情報源のように見せかけ、職員に電子メールの返信を送信したり、ウェブ リンクをクリックしたり、侵害されたウェブ サイトにデータを入力するように指示します。フィッシングを検知・防止する仕組みは、マルウェア対策ソリューションに含まれていることが多いです。 **その他の情報** フィッシングについては、以下をご参照ください。 *ナショナル・サイバー・セキュリティ・センター - フィッシング攻撃：あなたの事業体を守る* *米国サイバーセキュリティ＆インフラセキュリティ局- フィッシングサイトの報告。*

要件 6：　安全なシステムおよびソフトウェアの開発と維持

セクション
6.1 安全なシステムおよびソフトウェアを開発・維持するためのプロセスおよび仕組みが定義され、理解されている。
6.2 特注ソフトウェアおよびカスタムメイドのソフトウェアは安全に開発されている。
6.3 セキュリティの脆弱性を特定し、対処している。
6.4 一般公開されているウェブ アプリケーションは、攻撃から保護されている。
6.5 すべてのシステムコンポーネントの変更が安全に管理されている。

概要

悪意を持った行為者は、セキュリティの脆弱性を利用して、システムに特権的にアクセスすることができます。これらの脆弱性の多くは、ベンダが提供するセキュリティパッチによって修正され、システムを管理する主体によってインストールされなければならない。悪意のある個人や悪意のあるソフトウェアによるアカウントデータの搾取や侵害から保護するために、すべてのシステムコンポーネントにはすべての適切なソフトウェアパッチを適用しなければなりません。

適切なソフトウェアパッチとは、パッチが既存のセキュリティ設定と対立しないことを決定するために十分に評価されテストされたパッチのことです。特注ソフトウェアおよびカスタムソフトウェアについては、ソフトウェアライフサイクル（SLC）プロセスや安全なコーディング技術を適用することで、多くの脆弱性を回避することができます。

アカウントデータまたはカード会員データ環境（CDE） のセキュリティに影響を与える可能性のあるアプリケーションコード、システム構成、またはその他の構成データを格納するコードリポジトリは、PCI DSS 評価の適用範囲に含まれます。

PCI SSC が検証したソフトウェアおよびソフトウェアベンダの使用、ならびに PCI SSC のソフトウェア標準の使用が要件 6 のコントロールの充足にどのように役立つかについての情報は、9 ページの PCI DSS と PCI SSC のソフトウェア規格の関係 を参照してください。

PCI DSS 用語の定義については、付録 G を参照してください。

注：*要件 6 は、ソフトウェアを安全に開発するための 6.2 項を除き、すべてのシステムコンポーネントに適用されます。この要件は、カード会員データ環境（CDE）に含まれるか接続されるシステムコンポーネントで使用される特注ソフトウェアおよびカスタムソフトウェアにのみ適用されます。*

要件とテスト手順		ガイダンス
6.1 安全なシステムおよびソフトウェアを開発し、維持するためのプロセスおよび仕組みが定義され、理解されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 要件 6.1.1 は、要件 6 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 6 で呼び出された特定のポリシーや手順を定義することも重要ですが、それらが適切に文書化され、維持され、普及することも同様に重要です。 **グッドプラクティス** プロセス、技術、ビジネス目的の変化に対応するため、必要に応じてポリシーと手順を更新することが重要です。そのため、定期的な更新だけでなく、変更があった場合はできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、企業のセキュリティの目的および原則を定義するものです。運用手順は、活動の実行方法を記述し、一貫した方法で、ポリシーの目的に従って望ましい結果を達成するために従う統制、方法、プロセスを定義します。
6.1.1 要件 6 で特定されたすべてのセキュリティポリシーと運用手順が • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に知られている。	**6.1.1** 要件 6 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューします。	
カスタイマイズアプローチの目的		
要件 6 に含まれる活動を満たすための期待、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべての支援活動が繰り返し可能であり、一貫して適用され、経営者の意図に適合している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、システムは安全に維持されず、セキュリティレベルが低下します。 **グッドプラクティス** 役割と責任は、方針と手順の中で文書化されるか、または別の文書で管理されることができます。 役割と責任を伝える一環として、事業体は、担当者に与えられた役割と責任を受け入れ、理解することを認めさせることを検討することができます。 **例** 役割と責任を文書化する方法として、責任者、説明責任者、相談役、情報提供者を含む責任分担マトリックス（RACI マトリックスとも呼ばれる）があります。
6.1.2 要件 6 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**6.1.2.a** 文書を調査し、要件 6 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	6.1.2.b 要件 6 の活動の実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタイマイズアプローチの目的		
要件 6 のすべての活動を実行するための日常的な責任が割り当てられている。担当者は、これらの要件の成功、継続的な運用に責任を負う。		

要件とテスト手順		ガイダンス
6.2 特注・カスタムソフトウェアが安全に開発されている。		
定義されたアプローチの要件 **6.2.1** 特注ソフトウェアおよびカスタムソフトウェアは、以下のように安全に開発されている。 • 安全な開発のための業界標準やベストプラクティスに基づいていること。 • PCI DSS に準拠する（たとえば、安全な認証およびロギングなど）。 • ソフトウェア開発ライフサイクルの各段階において情報セキュリティの問題を考慮すること。 **カスタイマイズアプローチの目的** オーダーメイドおよびカスタムソフトウェアは、ソフトウェアライフサイクルを通じて PCI DSS および安全な開発プロセスに従って開発される。 **適用上の注意** これは、事業者のために、または事業者が事業者自身の使用のために開発したすべてのソフトウェアに適用される。これには、特注ソフトウェアおよびカスタムメイドのソフトウェアの両方が含まれる。サードパーティソフトウェアには適用されない。	**定義されたアプローチのテスト手順** **6.2.1** 文書化されたソフトウェア開発手順を調べ、この要件で指定されたすべての要素を含むプロセスが定義されていることを確認する。	**目的** ソフトウェア開発の要件定義、設計、分析、テストの各フェーズでセキュリティを考慮しないと、セキュリティの脆弱性が不注意または悪意を持って本番環境に導入される可能性があります。 **グッドプラクティス** 保存、送信、メモリ内など、機密データがアプリケーションでどのように扱われるかを理解することは、データを保護する必要がある場所を特定するのに役立ちます。 PCI DSS 要件を考慮してソフトウェアを開発し、後からソフトウェアを改修しようとするのではなく、設計時にその要件を満たすようにする必要があります。 **例** セキュアソフトウェアライフサイクル管理の方法論とフレームワークには、PCI セキュアソフトウェアフレームワーク, BSIMM、OPENSAMM、NIST、ISO、SAFECode の著作物が含まれます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.2.2 特注ソフトウェアおよびカスタムソフトウェアに従事するソフトウェア開発担当者は，少なくとも 12 カ月に 1 回，次のような訓練を受ける。 • 自分の職能および開発言語に関連するソフトウェアセキュリティについて。 • 安全なソフトウェア設計および安全なコーディング技法を含む。 • セキュリティテストツールを使用する場合、ソフトウェアの脆弱性を検出するためのツールの使用方法を含む。	**6.2.2.a** ソフトウェア開発手順を調査し、本要件で指定されたすべての要素を含む特注ソフトウェアおよびカスタムソフトウェアを開発するソフトウェア開発担当者のトレーニングのためのプロセスが定義されていることを確認する。	要件 6.2.4 で定義された手法を含むセキュアコーディング手法に精通したスタッフがいることで、不適切なコーディング手法によってもたらされるセキュリティ脆弱性の数を最小化することができます。
カスタイマイズアプローチの目的	**6.2.2.b** 研修記録を調査し、担当者にインタビューして、特注ソフトウェアおよびカスタムソフトウェアに従事するソフトウェア開発担当者が、本要件で指定されたすべての要素に従って、職務および開発言語に関連したソフトウェアセキュリティ研修を受けたことを確認する。	**グッドプラクティス**
ソフトウェア開発担当者は、安全な開発手法、ソフトウェアセキュリティ、および開発する言語、フレームワーク、またはアプリケーションに対する攻撃に関する知識を有している。担当者は、必要に応じて支援や指導を受けることができる。		開発者向けのトレーニングは、社内で行うことも、第三者が行うこともできます。 トレーニングには、使用する開発言語、安全なソフトウェア設計、安全なコーディング技術、コードの脆弱性を発見する技術／手法の使用、解決済みの脆弱性の再導入を防ぐプロセス、ソフトウェアの脆弱性を検出するための自動セキュリティテストツールの使用方法などが含まれるべきであるが、これらに限定されません。 業界で認められているセキュアコーディングの手法が変化した場合、事業体のコーディング手法と開発者のトレーニングは、新しい脅威に対応するために更新する必要がある場合があります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.2.3 特注ソフトウェアおよびカスタムソフトウェアは、潜在的なコーディングの脆弱性を特定し修正するために、実稼働または顧客にリリースする前に、以下のようにレビューされる。 • コードレビューでは、コードが安全なコーディングガイドラインに従って開発されていることを確認する。 • コードレビューでは、既存のソフトウェア脆弱性と新たに発生したソフトウェア脆弱性の両方を調査します。 • リリース前に適切な修正を実施する。	**6.2.3.a** 文書化されたソフトウェア開発手順を調べ、担当者にインタビューし、すべての特注ソフトウェアとおよびカスタムソフトウェアがこの要件で指定されたすべての要素に従ってレビューされることを要求するプロセスが定義されていることを確認する。	特注ソフトウェアおよびカスタムソフトウェアのセキュリティ脆弱性は、一般的に悪意のある人物によってネットワークにアクセスされ、アカウントデータを侵害されることがあります。 脆弱性のあるコードは、本番環境に導入またはリリースされた後に対処するのがはるかに困難であり、コストもかかります。リリース前に管理者による正式なレビューとサインオフを要求することで、コードが承認され、ポリシーと手順に従って開発されたことを確認することができます。
カスタイマイズアプローチの目的	**6.2.3.b** 特注ソフトウェアおよびカスタムソフトウェアの変更の証拠を調査し、コード変更がこの要件で指定されたすべての要素に従ってレビューされたことを確認する。	**グッドプラクティス** コードレビューでは、次のような項目を検討する必要があります。 • 文書化されていない機能（埋め込みツール、バックドア）の検索。 • ソフトウェアが外部コンポーネントの機能（ライブラリ、フレームワーク、API など）を安全に使用していることを確認する。例えば、暗号機能を提供するサードパーティライブラリを使用している場合、それが安全に統合されていることを確認する。
特注ソフトウェアおよびカスタムソフトウェアは、コーディングの脆弱性を悪用されることはない。		*(次ページに続く)*
適用上の注意		
コードレビューに関するこの要件は、システム開発ライフサイクルの一環として、すべての特注ソフトウェアおよびカスタムソフトウェア（内部向けおよび公共向けの両方）に適用される。		
(次ページに続く)		

要件とテスト手順		ガイダンス
公衆向けのウェブ アプリケーションも、PCI DSS 要件 6.4 で定義されているように、実装後に継続する脅威と脆弱性に対処するための追加コントロールの対象となる。 コードレビューは、手動または自動プロセスのいずれか、あるいは両方を組み合わせて実行することができない。		• 機密データがログに残らないよう、ログが正しく使用されているかを確認する。 • 要件 6.2.5 で特定された一般的なソフトウェア攻撃に関連する潜在的な脆弱性を含む可能性のある安全でないコード構造の分析。 • 論理的な脆弱性を検出するために、アプリケーションの動作をチェックすること。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.2.3.1 本番環境へのリリース前に、特注ソフトウェアおよびカスタムソフトウェアに対して手動コードレビューを実施する場合、コード変更は • コードレビュー技術やセキュアコーディングの実践に精通した、元のコード作成者以外の個人によってレビューされる。 • リリース前に管理者によってレビューされ、承認される。	**6.2.3.1.a** 本番環境へのリリース前に、特注ソフトウェアおよびカスタムソフトウェアに対して手動コードレビューを実施する場合、文書化されたソフトウェア開発手順を調べ、担当者にインタビューを行い、この要件に規定されたすべての要素に従って手動コードレビューを実施するためのプロセスが定義されていることを確認する。	コードレビューの経験があり、セキュアコーディングの実践に精通している原作者以外の人物にコードをレビューしてもらうことで、カード会員データのセキュリティに影響を与える可能性のあるセキュリティエラーまたはロジックエラーを含むコードが本番環境にリリースされる可能性を最小にすることができます。コードがレビューされたことを管理者に承認してもらうことで、プロセスが回避される可能性を制限することができます。
カスタイマイズアプローチの目的	**6.2.3.1.b** 特注ソフトウェアおよびカスタムソフトウェアに対する変更の証拠を調査し、担当者にインタビューして、この要件で指定されているすべての要素に従って手動コードレビューが実施されたことを確認する。	**グッドプラクティス**
手動コードレビューのプロセスは回避することができず、セキュリティ脆弱性の発見に効果的である。		正式なレビュー方法論とレビューチェックリストを持つことは、コードレビュープロセスの品質を向上させることが判明しています。
適用上の注意		コードレビューは疲れる作業です。このため、レビュアーが一度に少量のコードしかレビューしない場合に最も効果的です。
手動コードレビューは、知識のある内部の担当者または知識のある第三者の担当者によって実施することができる。 リリース管理に関する説明責任を正式に付与された個人で、オリジナルのコード作成者でもコードレビュー者でもない人は、管理者であるという基準を満たす。		コードレビューの効果を維持するためには、レビュアーの一般的な作業量を監視し、彼らが精通しているアプリケーションをレビューさせることが有益です。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		コードレビューは、手動または自動プロセスのいずれか、あるいは両方を組み合わせて実行することができます。 手動コードレビューにのみ依存している事業体は、新しい脆弱性が発見されたときや、新しい安全なコーディング方法が推奨された場合に、定期的なトレーニングを通じてレビュアーのスキルを維持することを保証する必要があります。 **その他の情報** *OWASP コードレビューガイド*を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
6.2.4 一般的なソフトウェア攻撃および関連する脆弱性を防止または軽減するために、ソフトウェアエンジニアリング技術またはその他の方法を定義し、ソフトウェア開発担当者が特注ソフトウェアおよびカスタムソフトウェアに対して使用している（ただし、以下に限定されない）。 • SQL、LDAP、XPath、またはその他のコマンド、パラメータ、オブジェクト、障害、インジェクションタイプの欠陥を含む、インジェクション攻撃。 • バッファ、ポインタ、入力データ、共有データを操作しようとする試みを含む、データおよびデータ構造に対する攻撃。 • 脆弱な、安全でない、または不適切な暗号の実装、アルゴリズム、暗号スイート、または操作モードを悪用しようとする試みを含む、暗号の使用に関する攻撃。 • 要件 6.3.1 に定義されているように、脆弱性特定プロセスで特定された「高リスク」の脆弱性を経由した攻撃。 *(次ページに続く)*	**6.2.4** 文書化された手順を調査し、ソフトウェア開発担当者にインタビューを行い、この要件で指定されている一般的なソフトウェア攻撃をすべて防止または軽減するために、ソフトウェア工学技術またはその他の方法が特注ソフトウェアおよびカスタムソフトウェアの開発者によって定義され、使用されていることを確認する。	**目的** 脆弱なコードにつながる一般的なエラーをソフトウェア開発プロセスのできるだけ早い段階で検出または防止することで、そのようなエラーが本番環境に出て危険にさらされる確率を低くすることができます。開発プロセスに形式的なエンジニアリング手法とツールを組み込むことで、これらのエラーを早期に発見することができます。この哲学は、「シフトレフト」と呼ばれることもあります。 **グッドプラクティス** 特注ソフトウェアおよびカスタムソフトウェアの両方について、事業者は、以下のような一般的なソフトウェア攻撃の防止または軽減に焦点を当てたコードを開発することを保証しなければなりません。 • 一般的なコーディングの脆弱性（バグ）を悪用しようとするもの。 • ソフトウェアの設計上の欠陥を利用しようとすること。 • 実装／設定の欠陥を利用しようとするもの。 • 列挙型攻撃 - 支払いにおいて積極的に悪用され、識別、認証、または認可の仕組みを悪用する自動的な攻撃。*PCI Perspectives ブログ記事 "アカウントテスト攻撃に注意* を参照してください。 *(次ページに続く)*

要件とテスト手順		ガイダンス
• ビジネスロジックに対する攻撃。API、通信プロトコルとチャンネル、クライアント側の機能、その他のシステム／アプリケーションの機能とリソースを操作して、アプリケーションの特徴と機能を悪用または回避しようとする試みを含む。これには、クロスサイトスクリプティング（XSS）やクロスサイトリクエストフォージェリ（CSRF）などが含まれる。 • 識別、認証、または認可の仕組みを迂回または悪用しようとする試み、あるいはそのような仕組みの実装における弱点を利用しようとする試みなど、アクセス制御の仕組みに対する攻撃。 **カスタマイズアプローチの目的** 特注ソフトウェアおよびカスタムソフトウェアは、一般的な攻撃や関連する脆弱性を悪用されることはない。 **適用に関する注意事項** これは、事業者のために、または事業者が事業者自身の使用のために開発したすべてのソフトウェアに適用される。これには、特注ソフトウェアおよびカスタムソフトウェアの両方が含まれる。サードパーティソフトウェアには適用されない。		ソフトウェア工学の技術やその他の方法を研究し文書化することは、ソフトウェア開発者がソフトウェアに組み込む機能または対策によって、さまざまなソフトウェア攻撃をどのように防止または軽減するかを定義するのに役立ちます。これには、識別／認証メカニズム、アクセス制御、入力検証ルーチンなどが含まれるかもしれない。開発者は、さまざまな種類の脆弱性と潜在的な攻撃について熟知し、コードを開発する際に潜在的な攻撃ベクトルを回避するための手段を用いる必要があります。 **例** 技術には、コードがチェックインされる開発サイクルの早い段階でコードをスキャンし、脆弱性が存在しないことを確認する自動化されたプロセスやプラクティスが含まれます。

要件とテスト手順		ガイダンス
6.3 セキュリティの脆弱性を特定し、対処している。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.3.1 セキュリティ脆弱性の特定と管理は、以下のように行っている。 • 新しいセキュリティ脆弱性は、国際的および国内のコンピュータ緊急対応チーム（CERT）からの警告を含む、業界で認知されたセキュリティ脆弱性情報源を使用して特定される。 • 脆弱性は、業界のベストプラクティスと潜在的な影響の考慮に基づいて、リスクランクが割り当てられている。 • リスクランキングでは、最低限、高リスクまたは環境にとって重要であると考えられるすべての脆弱性を特定する。 • 特注ソフトウェアおよびカスタムソフトウェア、サードパーティソフトウェア（OS やデータベースなど）に対する脆弱性が対象となる。	**6.3.1.a** セキュリティ脆弱性の特定と管理のためのポリシーと手順を調べ、この要件で指定されているすべての要素に従ってプロセスが定義されていることを確認する。	リスクを分類（例えば、重要、高、中、低）することにより、事業体は最もリスクの高い項目をより迅速に特定し、優先順位をつけて対処し、最大のリスクをもたらす脆弱性が悪用される可能性を低減することができます。
カスタマイズアプローチの目的	**6.3.1.b** 担当者にインタビューし、文書を調査し、プロセスを観察して、この要件で指定されたすべての要素に従ってセキュリティ脆弱性が識別され管理されていることを確認する。	**グッドプラクティス** 脆弱性を評価し、リスク評価を行う方法は、事業体の環境やリスク評価戦略によって異なります。 事業体がリスクランキングを割り当てる場合、事業体に関連する脆弱性のリスクを正確に描写し、事業体が割り当てた適切な解決のための優先順位に変換する、公式で客観的かつ正当な方法を使用することを検討する必要があります。 事業体の脆弱性管理プロセスは、他の管理プロセス（例えば、リスク管理、変更管理、パッチ管理、インシデント対応、アプリケーションセキュリティ、およびこれらのプロセスの適切な監視と記録）と統合される必要があります。これにより、すべての脆弱性が適切に識別され、対処されるようになります。プロセスは、脆弱性の継続的な評価をサポートする必要があります。
アカウントデータまたはカード会員データ環境（CDE）のセキュリティに影響を与える可能性のある新しいシステムおよびソフトウェアの脆弱性を監視し、カタログ化し、リスク評価する。		
(次ページに続く)		*(次ページに続く)*

要件とテスト手順		ガイダンス
適用に関する注意事項 この要件は、要件 11.3.1 および 11.3.2 で実施される脆弱性スキャンによって達成されるものではなく、また同じものでもない。この要件は、脆弱性情報の業界ソースを積極的に監視し、事業体が各脆弱性に関連付けられるリスクランキングを決定するためのプロセスである。		例えば、当初は低リスクと認識された脆弱性が、後に高リスクとなる可能性があります。さらに、個々には低リスクまたは中リスクとみなされる脆弱性が、同じシステム上に存在する場合、または低リスクのシステム上で悪用され、カード会員データ環境（CDE）へのアクセスにつながる場合、集合的に高リスクまたは重大リスクを引き起こす可能性があります。 **例** 早急なパッチやアップデートが必要な緊急の脆弱性について、事業体に通知するアラートを発行する事業体には、国のコンピュータ緊急対応チーム（CERT）やベンダがあります。 脆弱性のランク付けの基準としては、FIRST（インシデントレスポンスとセキュリティチームのフォーラム）や CERT からの警告で特定された脆弱性の重要度、CVSS スコアの考慮、ベンダによる分類、影響を受けるシステムのタイプなどが考えられます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		その他の情報 信頼できる脆弱性情報源としては、ベンダのウェブ サイト、業界のニュースグループ、メーリングリストなどがあります。ソフトウェアを社内で開発している場合、社内の開発チームは、社内で開発されたアプリケーションに影響を及ぼす可能性のある新しい脆弱性に関する情報源も考慮する必要があります。また、新しい脆弱性を確実に特定する方法として、異常な動作の検出時に自動的に認識し警告するソリューションもあります。このプロセスでは、広く公開されている脆弱性だけでなく、これまで知られていなかった脆弱性を標的とする「ゼロデイ」攻撃も考慮する必要があります。 特注ソフトウェアおよびカスタムソフトウェアについては、ライブラリ、フレームワーク、コンパイラ、プログラミング言語などに関する情報を、信頼できる公開情報源（例えば、特別なリソースやコンポーネント開発者のリソースなど）から入手することができます。また、サードパーティのコンポーネントを独自に解析し、脆弱性を特定することもあります。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		自社開発ソフトウェアの管理については、外部よりそのような情報を受け取ることができる。事業体は、第三者が脆弱性情報を事業体に連絡できるように、情報を（例えばウェブサイトに）掲載する「バグバウンティ」プログラムの利用を検討することができます。外部の情報源としては、独立した調査機関や、特定された脆弱性について事業体に報告する企業などが考えられ、共通脆弱性評価システム（CVSS）、OWASP リスク評価手法などの情報源が考えられます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 事業体の特注・カスタムソフトウェア、および事業体の特注・カスタムソフトウェアに組み込まれているサードパーティソフトウェアをすべて特定し、リストアップすることで、事業体は脆弱性とパッチを管理することができます。 事業体のソフトウェアに組み込まれたサードパーティコンポーネント（ライブラリ、API などを含む）の脆弱性は、それらのアプリケーションを攻撃に対して脆弱にするものでもあります。事業体のソフトウェアで使用されているサードパーティコンポーネントを把握し、既知の脆弱性に対処するためのセキュリティパッチの利用可能性を監視することは、ソフトウェアのセキュリティを確保する上で非常に重要です。 **グッドプラクティス** 事業体のインベントリには、サポートされる実行プラットフォームまたは環境、サードパーティライブラリ、サービス、その他必要な機能を含め、すべてのペイメントソフトウェアコンポーネントと依存関係を網羅する必要があります。 ソフトウェア構成分析ツール、アプリケーション発見ツール、モバイルデバイス管理など、ソフトウェアインベントリの管理に役立つさまざまな種類のソリューションがあります。
6.3.2 特注ソフトウェアおよびカスタムソフトウェア、並びに特注ソフトウェアおよびカスタムソフトウェアに組み込まれたサードパーティソフトウェアコンポーネントのインベントリを維持し、脆弱性およびパッチ管理を容易にする。	**6.3.2.a** 特注ソフトウェアおよびカスタムソフトウェア、並びに特注ソフトウェアおよびカスタムソフトウェアに組み込まれた第三者ソフトウェア部品の目録が維持されていること、並びにその目録が脆弱性の特定および対処に使用されていることを確認するために、文書を調査し、担当者にインタビューする。	
	6.3.2.b 第三者のソフトウェア部品を統合した特注ソフトウェアおよびカスタムソフトウェアを含むソフトウェア文書を調査し、インベントリと比較して、インベントリに特注・カスタムソフトウェアおよび第三者のソフトウェア部品が含まれていることを確認する。	
カスタマイズアプローチの目的 サードパーティソフトウェアコンポーネントの既知の脆弱性を、特注ソフトウェアおよびカスタムソフトウェアで悪用できないようにする。		
適用に関する注意事項 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.3.3 すべてのシステムコンポーネントは、以下のように適用可能なセキュリティパッチ／アップデートをインストールすることで、既知の脆弱性から保護されている。 • 重要または高セキュリティなパッチ/アップデート（要件 6.3.1 のリスクランク付けプロセスに従って識別）がリリース後 1 カ月以内にインストールされている。 • 重要または高セキュリティのパッチ／アップデートは、リリース後 1 カ月以内にインストールされる。 • その他の適用可能なセキュリティパッチ／アップデートが、事業体の定める適切な期間内（たとえば、リリースから 3 カ月以内）にインストールされる。	**6.3.3.a** ポリシーと手順を調査し、この要件で指定されたすべての要素に従って、該当するセキュリティパッチ／アップデートをインストールすることによって脆弱性に対処するためのプロセスが定義されていることを確認する。 **6.3.3.b** システムコンポーネントと関連ソフトウェアを調べ、インストールされているセキュリティパッチ／更新プログラムのリストを最新のセキュリティパッチ／更新プログラムと比較し、この要件で指定されているすべての要素に従って脆弱性が対処されていることを確認する。	新しいエクスプロイトは常に発見されており、これまで安全とされてきたシステムに対しても攻撃を許してしまう可能性があります。重要なシステムに最新のセキュリティパッチ／アップデートをできるだけ早く導入しなければ、悪意のある行為者がこれらのエクスプロイトを利用してシステムを攻撃したり、機能を停止させたり、機密データにアクセスすることが可能になります。 **グッドプラクティス** 重要インフラに対するセキュリティパッチ／アップデートの優先順位を決めることで、優先度の高いシステムやデバイスがパッチリリース後できるだけ早く脆弱性から保護されるようにします。 事業体のパッチ適用間隔は、要件 6.3.1 に従って、脆弱性の再評価とその後の脆弱性の重要性の変化を考慮する必要があります。例えば、当初は低リスクと認識された脆弱性が、後に高リスクとなる可能性があります。さらに、個別に低リスクまたは中リスクとみなされた脆弱性が、同じシステム上に存在する場合、または低リスクのシステム上で悪用され、カード会員データ環境（CDE）へのアクセスにつながる場合、集合的に高リスクまたは重大なリスクを引き起こす可能性があります。
カスタマイズアプローチの目的		
既知の脆弱性を悪用したシステムコンポーネントの侵入が不可能であること。		

要件とテスト手順		ガイダンス
6.4 一般公開されているウェブ アプリケーションは攻撃から保護されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.4.1 一般公開されている ウェブ アプリケーションについては、新たな脅威や脆弱性に継続的に対処し、既知の攻撃から以下のように保護する。 • 手動または自動のアプリケーション脆弱性セキュリティ評価ツールまたは手法により、公開用ウェブアプリケーションを以下のようにレビューする。 – 少なくとも 12 カ月に一度、および大幅な変更があった後に実施する。 – アプリケーションのセキュリティを専門とする事業体によるものであること。 – 少なくとも、要件 6.3.6 のすべての一般的なソフトウェア攻撃を含む。 – すべての脆弱性が要件 6.2.1 に従ってランク付けされている。 – すべての脆弱性が修正される。 – 修正後、アプリケーションを再評価する。 *(次ページに続く)*	**6.4.1** 一般公開されているウェブ アプリケーションの場合、以下のように必要な方法のいずれかが実施されていることを確認する。 • 手動または自動の脆弱性セキュリティ評価ツールまたは方法が使用されている場合、文書化されたプロセスを調べ、担当者にインタビューし、アプリケーションセキュリティ評価の記録を調べて、ツール／方法に固有のこの要件のすべての要素に従って公衆向けのウェブ アプリケーションがレビューされていることを確認する。 **または** ウェブ ベースの攻撃を継続的に検出および防止する自動化された技術的ソリューションがインストールされている場合、システム構成設定と監査ログを調査し、担当者にインタビューして、自動化された技術的ソリューションがソリューションに固有のこの要件のすべての要素に準拠してインストールされていることを確認する。	一般公開されているウェブ アプリケーションとは、内部利用だけでなく、一般に公開されるウェブ アプリケーションのことです。これらのアプリケーションは攻撃者の主要なターゲットであり、不適切にコーディングされたウェブアプリケーションは、攻撃者が機密データやシステムにアクセスするための容易な経路を提供します。 **グッドプラクティス** 手動または自動の脆弱性セキュリティ評価ツールまたは手法により、アプリケーションの脆弱性をレビューおよび／またはテストします。 一般的な評価ツールには、ウェブアプリケーションの保護に関する自動分析を行う専用のウェブスキャナーがあります。 自動化された技術的ソリューションを使用する場合、検出された攻撃を軽減できるように、ソリューションによって生成されたアラートにタイムリーに対応するプロセスを含めることが重要です。 *(次ページに続く)*

要件とテスト手順		ガイダンス
または • 以下のように、ウェブ ベースの攻撃を継続的に検出し、防止する自動化された技術的なソリューション（複数可）を設置すること。 – ウェブベースの攻撃を検知・防止するために、一般公開されるウェブアプリケーションの前に設置されていること。 – アクティブに実行され、該当する場合は最新の状態に更新されていること。 – 監査ログを生成していること。 – ウェブベースの攻撃をブロックするか、アラートを生成して直ちに調査するように設定されている。 **カスタマイズアプローチの目的** 一般公開されているウェブ アプリケーションは、悪意のある攻撃から保護されている。 **適用に関する注意事項** この評価は、要件 11.3.1 および 11.3.2 で実施した脆弱性スキャンとは異なる。 この要件は、要件 6.4.2 が発効する 2025 年 3 月 31 日以降、要件 6.4.2 に置き換えられる。		**例** 一般公開されているウェブ アプリケーションの前に設置し、すべてのトラフィックをチェックするウェブ アプリケーションファイアウォール（WAF）は、ウェブ ベースの攻撃（たとえば、要件 6.2.4 に含まれる攻撃）を検出して防止する自動技術ソリューションの一例です。WAF は、アプリケーション層で非本質的なトラフィックをフィルタリングおよびブロックします。WAF を適切に設定することで、不適切にコーディングまたは設定されたアプリケーションに対するアプリケー ション層からの攻撃を防止することができます。 自動化された技術ソリューションのもう一つの例は、RASP（ランタイムアプリケーションセルフプロテクション）技術である。RASP ソリューションは、正しく実装された場合、実行中のソフトウェアによる異常な動作を検出し、ブロックすることができます。WAF は通常、アプリケーションの周囲を監視しますが、RASP ソリューションはアプリケーション内の動作を監視し、ブロックします。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
6.4.2 一般公開されているウェブ アプリケーションについては、ウェブ ベースの攻撃を継続的に検知・防止する自動化された技術的ソリューションを導入しており、少なくとも以下の条件を備えている。 • 一般公開されているウェブアプリケーションの前にインストールされ、ウェブベースの攻撃を検知・防止するように設定されている。 • アクティブに実行され、該当する場合は最新の状態に更新されていること。 • 監査ログを生成していること。 • ウェブ ベースの攻撃をブロックするか、アラートを生成して直ちに調査するように設定されている。	**6.4.2** 一般公開されているウェブ アプリケーションについては、システム構成設定と監査ログを調査し、担当者にインタビューして、ウェブ ベースの攻撃を検出および防止する自動化された技術ソリューションが、この要件で指定されたすべての要素に従って配置されていることを確認する。	**目的** 一般公開されているウェブアプリケーションは、攻撃者の主要なターゲットであり、不適切にコーディングされたウェブアプリケーションは、攻撃者が機密データやシステムにアクセスするための容易な経路を提供します。 **グッドプラクティス** 自動化された技術的ソリューションを使用する場合、検出された攻撃を軽減できるように、ソリューションによって生成されたアラートにタイムリーに対応するプロセスを含めることが重要です。このようなソリューションは、ブルートフォース攻撃や列挙型攻撃に対する軽減を自動化するために、例えばレート制限コントロールのように使用することもできます。

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 一般公開されているウェブ アプリケーションは、悪意のある攻撃からリアルタイムに保護されている。 **適用に関する注意事項** この新しい要件は、発効日に到達した時点で、要件 6.4.1 に置き換わる。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		**例** ウェブ アプリケーションファイアウォール（WAF）は、オンプレミスまたはクラウドベースで、一般公開されている ウェブ アプリケーションの前に設置され、すべてのトラフィックをチェックします。これは、ウェブ ベースの攻撃（たとえば、要件 6.2.4 に含まれる攻撃）を検出して防止する自動化技術ソリューションの一例です。 *(次ページに続く)* WAF は、アプリケーション層で非本質的なトラフィックをフィルタリングおよびブロックします。WAF を適切に設定することで、不適切にコーディングまたは設定されたアプリケーションに対するアプリケー ション層からの攻撃を防止することができます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.4.3 消費者のブラウザに読み込まれ実行されるすべての決済ページスクリプトは、以下のように管理される。 • 各スクリプトが認可されていることを確認するための方法が実装されている。 • 各スクリプトの整合性を保証するための方法が実装されている。 • すべてのスクリプトのインベントリが、それぞれのスクリプトが必要な理由を説明した文書とともに維持される。	**6.4.3.a** ポリシーと手順を調査し、消費者のブラウザに読み込まれて実行されるすべての支払ページスクリプトを管理するためのプロセスが、この要件で指定されたすべての要素に従って定義されていることを確認する。	決済ページでロードされ実行されるスクリプトは、事業体が知らないうちにその機能が変更されることがあり、また追加の外部スクリプト（例えば広告やトラッキング、タグ管理システムなど）をロードする機能を持つこともあります。 このような一見無害なスクリプトは、潜在的な攻撃者が消費者ブラウザからカード会員データを読み取り、流出させる悪意のあるスクリプトをアップロードするために使用される可能性があります。 そのようなスクリプトのすべての機能が支払ページの操作に必要であると理解されるようにすることで、改ざんされる可能性のあるスクリプトの数を最小限に抑えることができます。 スクリプトが明示的に許可されていることを確認することで、適切な管理承認なしに不要なスクリプトがペイメントページに追加される可能性を減らすことができます。 スクリプトの改ざんを防止する技術を使用すると、スクリプトが修正されて、決済ページからカード会員データをスキミングするなどの不正な動作が実行される確率を最小にできます。 *(次ページに続く)*
カスタマイズアプローチの目的	**6.4.3.b** 担当者にインタビューを行い、インベントリ記録およびシステム構成を調査し、消費者のブラウザに読み込まれ実行されるすべての支払ページスクリプトが、この要件で指定されているすべての要素に従って管理されていることを確認する。	
消費者のブラウザでレンダリングされる決済ページには、未許可のコードは存在できない。		
適用に関する注意事項		
この要件は、事業体の環境からロードされるすべてのスクリプトと、サードパーティおよび第 4 のパーティからロードされるスクリプトに適用される。 この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
		グッドプラクティス スクリプトは、手動または自動（例：ワークフロー）プロセスによって承認される場合があります。 決済ページがインラインフレーム（IFRAME）に読み込まれる場合、親ページのコンテンツセキュリティポリシー（CSP）を使用して決済ページを読み込める場所を制限すると、未承認コンテンツが決済ページに置き換えられることを防ぐことができます。 **定義** この要件における「必要」とは、事業体による各スクリプトのレビューで、決済取引を受け入れる決済ページの機能に必要な理由が正当化され確認されることを意味します。 **例** スクリプトの完全性は、以下のようないくつかの異なるメカニズムによって強制することができる（ただし、これらに限定されない）。 • サブリソースの整合性（SRI）：コンシューマーブラウザは、スクリプトが改ざんされていないことを検証することができます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		• CSP：コンシューマ ブラウザがスクリプトをロードして アカウントデータ を送信できる場所を限定します。 • 悪意のあるスクリプトの実行を防ぐことができる、独自のスクリプトまたはタグ管理システム。

要件とテスト手順		ガイダンス
6.5 すべてのシステムコンポーネントの変更が安全に管理されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.5.1 本番環境におけるすべてのシステムコンポーネントの変更は、以下を含む確立された手順に従って行われる。 • 変更の理由および説明 • セキュリティ上の影響に関する文書化 • 権限のある当事者による文書化された変更承認 • 変更がシステムセキュリティに悪影響を及ぼさないことを検証するためのテスト。 • 特注ソフトウェアおよびカスタムソフトウェアの変更については、すべてのアップデートが本番環境に導入される前に、要件 6.2.4 に準拠しているかどうかテストされる。 • 障害に対処し、安全な状態に戻すための手順。	**6.5.1.a** 文書化された変更管理手順を調べ、本番環境におけるすべてのシステムコンポーネントの変更について、この要件で指定されたすべての要素を含む手順が定義されていることを確認する。	本番環境におけるすべての変更（システムコンポーネントの追加、削除、修正を含む）には、変更管理手順が適用されなければなりません。変更の理由と変更の内容を文書化し、関係者がその変更の必要性を理解し、合意することが重要です。同様に、変更の影響を文書化することで、影響を受けるすべての関係者が、処理の変更に対して適切な計画を立てることができます。
カスタマイズアプローチの目的	**6.5.1.b** システムコンポーネントに対する最近の変更を調査し、それらの変更を関連する変更管理文書に遡って追跡する。調査した各変更について、その変更がこの要件で指定されたすべての要素に従って実装されていることを確認する。	**グッドプラクティス**
すべての変更が追跡され、承認され、影響とセキュリティについて評価され、システムコンポーネントのセキュリティへの意図しない影響を避けるために変更が管理されている。		権限のある当事者による承認は、変更が正当であり、その変更が事業体によって承認されたことを確認するものです。変更は、変更の影響を理解するための適切な権限と知識を持つ個人によって承認されるべきです。 事業者による徹底的なテストは、変更の実施によって環境のセキュリティが低下しないこと、および、既存のすべてのセキュリティ管理が変更後も維持されるか、変更後に同等またはより強力なセキュリティ管理に置き換えられることを確認するものである。実施すべき具体的なテストは、変更の種類と影響を受けるシステムコンポーネントによって異なります。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		それぞれの変更について、失敗した場合に対処する手順を文書化し、変更が失敗した場合やアプリケーションやシステムのセキュリティに悪影響を及ぼす場合に、安全な状態に戻す方法を示すことが重要です。これらの手順により、アプリケーションまたはシステムを以前の安全な状態に戻すことができます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.5.2 大幅な変更が完了したら、該当するすべての PCI DSS 要件がすべての新規または変更されたシステムおよびネットワークに適用されることを確認し、該当する文書を更新する。	**6.5.2** 大幅な変更に関する文書を調査し、担当者にインタビューし、影響を受けるシステム／ネットワークを観察して、事業体は該当するすべての PCI DSS 要件がすべての新規または変更されたシステムおよびネットワークに適用されていることを確認し、該当する場合は文書が更新されたことを確認する。	大幅な変更を分析するプロセスを持つことは、適用範囲内の環境内で追加または変更されたシステムまたはネットワークに適切なすべての PCI DSS コントロールが適用され、環境を保護するための PCI DSS 要件が引き続き満たされることを保証するために役立ちます。 **グッドプラクティス** この検証を変更管理プロセスに組み込むことで、デバイスのインベントリや構成基準を最新の状態に保ち、必要に応じてセキュリティ管理を適用することができるようになります。 **例** 影響を受ける可能性のある適用可能な PCI DSS 要件には、以下のものが含まれますが、これらに限定されるものではありません。 • ネットワーク図およびデータフロー図は、変更を反映するために更新されます。 • システムは構成基準に従って構成され、すべてのデフォルトパスワードは変更され、不要なサービスは無効化されます。 *(次ページに続く)*
カスタマイズアプローチの目的		
大幅な変更後に、すべてのシステムコンポーネントが該当する PCI DSS 要件に準拠していることを検証する。		
適用に関する注意事項		
これらの大幅な変更は、要件 12.5.2 に従って、事業体の年次 PCI DSS 適用範囲確認アクティビティでも記録および反映される必要がある。		

要件とテスト手順		ガイダンス
		• システムは、ファイル整合性監視（FIM）、アンチマルウェア、パッチ、監査ログなど、必要なコントロールで保護されています。 • 機密認証データは保存せず、すべてのアカウントデータの保存は文書化され、データ保存ポリシーと手順に組み込まれています。 • 新しいシステムは、四半期ごとの脆弱性スキャンプロセスに含まれます。 • 要件 11.3.1.3 および要件 11.3.2.1 に従った大幅な変更後に、内部および外部の脆弱性のスキャンが実施されます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** プレ本番環境は常に変化しているため、本番環境よりも安全性が低いことが多いです。 **グッドプラクティス** どの環境がテスト環境なのか、開発環境なのか、また、これらの環境がネットワークやアプリケーションのレベルでどのように相互作用するのか、事業体は明確に理解する必要があります。 **定義** プレ本番環境には、開発、テスト、ユーザ受入テスト（UAT）などがあります。テストや開発を促進するために本番環境のインフラストラクチャが使用される場合でも、本番環境は、プレ本番環境でのアクティビティの結果としてもたらされる脆弱性が本番システムに悪影響を与えないように、プレ本番環境の機能から（論理的または物理的に）分離する必要があります。
6.5.3 プレ本番環境は本番環境から分離され、その分離はアクセス制御によって強制される。	**6.5.3.a** ポリシーおよび手順を調査し、プレ本番環境と本番環境を分離するためのプロセスが、分離を強制するアクセス制御によって定義されていることを確認する。	
	6.5.3.b ネットワークドキュメントおよびネットワークセキュリティコントロールの構成を調査し、プレ本番環境が本番環境から分離されていることを確認する。	
カスタマイズアプローチの目的 プレ本番環境は、本番環境にリスクや脆弱性を持ち込むことはできない。	**6.5.3.c** アクセス制御の設定を調査し、プレ本番環境と本番環境の分離を実施するためのアクセス制御が実施されていることを確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **6.5.4** 本番環境とプレ本番環境の間で役割と機能を分離し、レビューおよび承認された変更のみを導入することで説明責任を果たす。	**定義されたアプローチのテスト手順** **6.5.4.a** ポリシーおよび手順を調査し、レビューおよび承認された変更のみを導入することで説明責任を果たすために、役割および機能を分離するためのプロセスが定義されていることを確認する。 **6.5.4.b** プロセスを観察し、担当者にインタビューして、実装されたコントロールによって役割と機能が分離され、レビューおよび承認された変更のみを導入することで説明責任が果たされることを確認する。	**目的** 本番環境とプレ本番環境で役割と機能を分ける目的は、本番環境とアカウントデータにアクセスできる担当者の数を減らし、それによってデータやシステムコンポーネントへの不正な、意図的でない、または不適切なアクセスのリスクを最小限に抑え、アクセスがビジネス上必要な個人に確実に制限されるようにすることです。 このコントロールの意図は、重要なアクティビティを分離して監視とレビューを行い、エラーを発見し、詐欺や盗難の可能性を最小限に抑えることです（アクティビティを隠すためには、2 人の人間が共謀する必要があるため）。 役割と機能を分離することは、職務の分離とも呼ばれ、企業の資産を保護するための重要な内部統制の概念です。
カスタマイズアプローチの目的 プレ本番環境と本番環境でのアクティビティを区別する職務上の役割と責任が定義され、管理されており、不正な、意図的でない、または不適切な行為のリスクが最小化されること。		
適用に関する注意事項 個人が複数の役割や機能を果たすような限られた担当者の環境では、説明責任を果たすための手続き的な管理を追加することで、これと同じ目標を達成することができる。たとえば、開発者は管理者でもあり、開発環境では高い権限を持つ管理者レベルのアカウントを使用し、開発者の役割では、本番環境にはユーザレベルのアクセス権を持つ別のアカウントを使用することができる。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
6.5.5 実際の PAN はプレ本番環境では使用してはならない。ただし、プレ本番環境が カード会員データ環境（CDE） に含まれ、適用されるすべての PCI DSS 要件に従って保護されている場合はこの限りではない。	**6.5.5.a** ポリシーと手順を調べて、プレ本番環境で実際の PAN を使用しないためのプロセスが定義されていることを確認する。ただし、 それらの環境が カード会員データ環境（CDE） 内にあり、該当するすべての PCI DSS 要件に従って保護されている場合はこの限りでない。	**目的** 保護された カード会員データ環境（CDE） の外部で実際の PAN を使用すると、悪意のある個人にカード会員データに不正にアクセスする機会を与えかねません。 **グッドプラクティス** 事業体は、特定の定義されたテスト目的のために厳密に必要な場合のみ、プレ本番環境に実際の PAN を保管し、使用後はそのデータを安全に削除することで、PAN の保管を最小限に抑えることができます。 テスト用に特別に設計された PAN が必要な場合は、アクワイアラから入手することができます。 **定義** 実際の PAN とは、決済取引に使用される可能性のある有効な PAN（テスト PAN ではない）のことです。また、ペイメントカードの有効期限が切れると、同じ PAN が別の有効期限で再利用されることがよくあります。すべての PAN は、PCI DSS の範囲から除外する前に、支払取引を行うことができないことを確認する必要があります。PAN が実際の PAN ではないことを確認するのは、事業体の責任です。
	6.5.5.b テストプロセスを観察し、担当者にインタビューして、プレ本番環境で実際の PAN が使用されていないことを確認する手順が実施されていることを確認する。ただし、これらの環境が カード会員データ環境（CDE） 内にあり、該当するすべての PCI DSS 要件に従って保護されている場合はこの限りでない。	
カスタマイズアプローチの目的 カード会員データ環境（CDE）外のプレ本番環境に実際の PAN を存在させない。	**6.5.5.c** プレ本番環境のテストデータを検証し、プレ本番環境で実際の PAN が使用されていないことを確認する。ただし、これらの環境が カード会員データ環境（CDE） 内にあり、該当するすべての PCI DSS 要件に従って保護されている場合はこの限りではない。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.5.6 テストデータおよびテストアカウントは、システムの本番稼動前にシステムコンポーネントから削除される。	**6.5.6.a** システムの本番稼動前に、システムコンポーネントからテストデータおよびテストアカウントを削除するためのプロセスが定義されていることを確認するために、ポリシーおよび手続を調査する。	このデータは、アプリケーションやシステムの機能に関する情報を与えてしまう可能性があり、許可されていない個人がシステムにアクセスするために悪用する可能性があります。このような情報を所持していると、システムおよび関連するアカウントデータの侵害が容易になる可能性があります。
	6.5.6.b 既製ソフトウェアと社内アプリケーションの両方のテストプロセスを観察し、担当者にインタビューして、システムの本番稼働前にテストデータおよびテストアカウントが削除されていることを確認する。	
カスタマイズアプローチの目的	**6.5.6.c** 最近インストールまたは更新された既成ソフトウェアおよび社内アプリケーションのデータおよびアカウントを調べ、本番システムにテストデータまたはテストアカウントがないことを確認する。	
テストデータやテストアカウントは本番環境には存在できない。		

強固なアクセス制御の実施

*要件 **7**：　　システムコンポーネントおよびカード会員データへのアクセスを、業務上必要な適用範囲（**Need to Know**）によって制限する*

セクション	
7.1	業務上必要なシステムコンポーネントとカード会員データへのアクセスを制限するためのプロセスと仕組みが定義され、理解されている。
7.2	システムコンポーネントおよびデータへのアクセス権が適切に定義され、割り当てられている。
7.3	システムコンポーネントおよびデータへのアクセスは、アクセス制御システムを介して管理されている。

概要

アクセス制御のルールや定義が有効でないため、権限のない個人が重要なデータやシステムにアクセスする可能性があります。重要なデータへのアクセスを許可された者のみが行えるようにするには、業務上必要な適用範囲（Need to Know）に基づいて、また職務上の責任に従ってアクセスを制限するシステムとプロセスを導入する必要があります。

「アクセス」または「アクセス権」は、ユーザにシステム、アプリケーション、およびデータへのアクセスを提供するルールによって作成され、「権限」は、ユーザがそのシステム、アプリケーション、またはデータに関連して特定のアクションまたは機能を実行することを許可します。例えば、あるユーザが特定のデータへのアクセス権を持っていても、そのデータを読むだけなのか、それとも変更や削除もできるのかは、そのユーザに与えられた権限によって決まります。

「Need to Know」とは、業務に必要な最小限のデータのみにアクセスできることです。

「最小限の権限」とは、業務を遂行するために必要な最小限の権限のみを提供することです。

これらの要件は、従業員、請負業者、コンサルタント、社内外のベンダやその他の第三者（例えば、サポートや保守サービスを提供するため）のユーザアカウントおよびアクセスに適用されます。また、企業が使用するアプリケーションおよびシステムアカウント（「サービスアカウント」とも呼ばれる）にも一定の要件が適用されます。

これらの要件は、消費者（カード会員）には適用されません。

PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
7.1 業務上知る必要のあるシステムコンポーネントおよびカード会員データへのアクセスを制限するための プロセスおよびメカニズムが定義され、理解されている。		
定義されたアプローチの要件 **7.1.1** 要件 7 で特定されたすべてのセキュリティポリシーと運用手順がある。 • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に知られている。 **カスタマイズアプローチの目的** 要件 7 に含まれる活動を満たすための期待されること、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべてのサポートアクティビティが繰り返し可能であり、一貫して適用され、経営者の意図に適合している。	**定義されたアプローチのテスト手順** **7.1.1** 要件 7 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューする。	**目的** 要件 7.1.1 は、要件 7 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 7 で呼び出された特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及していることを確認することも同様に重要です。 **グッドプラクティス** プロセス、技術、事業目的の変化に対応するため、必要に応じてポリシーや手順を更新することが重要です。そのため、定期的な更新だけでなく、変更が発生したらできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、事業体のセキュリティの目的および原則を定義するものです。運用手順は、アクティビティの実行方法を記述し、一貫した方法で、ポリシーの目的に従って望ましい結果を達成するために従う統制、方法、プロセスを定義します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要なアクティビティが行われない可能性があります。 **グッドプラクティス** 役割と責任は、ポリシーと手順の中で文書化されるか、または別の文書で管理されるかもしれません。 役割と責任を伝える一環として、事業体は担当者が与えられた役割と責任を受け入れ理解したことの確認を検討することができます。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担マトリックス（RACI マトリックスとも呼ばれる）があります。
7.1.2 要件 7 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**7.1.2.a** 文書を調査し、要件 7 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	7.1.2.b 要件 7 の活動実施に責任を持つ担当者にインタビューを行い、役割と責任がそのように割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 7 のすべての活動を実行するための日常的な責任が割り当てられている。担当者は、これらの要件の成功、継続的な運用に責任を負う。		

要件とテスト手順		ガイダンス
7.2 システムコンポーネントやデータへのアクセスが適切に定義され、割り当てられている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
7.2.1 アクセス制御モデルが定義され、以下のようにアクセスを許可することが含まれる。 • 事業体のビジネスおよびアクセスの必要性に応じた適切なアクセス。 • ユーザの職務分類および機能に基づく、システムコンポーネントおよびデータリソースへのアクセス。 • 職務上の機能を果たすために必要な最小限の権限（例えば、ユーザ、管理者）。	**7.2.1.a** 文書化されたポリシーと手順を調べ、担当者にインタビューして、アクセス制御モデルがこの要件で指定されたすべての要素に従って定義されていることを確認する。	**目的** 事業体の技術やアクセス制御の考え方に適したアクセス制御モデルを定義することで、一貫性のある均一なアクセス割り当て方法を支援し、過剰な権利の付与などの誤りの可能性を低減することができます。 **グッドプラクティス** アクセスニーズを定義する際に考慮すべき要因として、職務分離の原則があります。この原則は、不正行為やリソースの誤用・盗難を防止するためのものです。例えば、1）ミッションクリティカルな機能と情報システムのサポート機能を異なる個人および／または機能に分割する、2）情報システムのサポートアクティビティを異なる機能／個人（例えば、システム管理、プログラミング、構成管理、品質保証およびテスト、ネットワークセキュリティ）が行うように役割を定める、3）アクセス制御機能を管理するセキュリティ担当者が監査機能を管理しないようにする、などです。 一人の個人が管理およびセキュリティ運用のような複数の機能を実行する環境では、独立したチェックポイントなしに、一人の個人がプロセスのエンドツーエンドを制御することがないように、職務を割り当てることができます。 *(次ページに続く)*
カスタマイズアプローチの目的	**7.2.1.b** アクセス制御モデルの設定を調べ、この要件で指定されたすべての要素に従ってアクセスニーズが適切に定義されていることを確認する。	
アクセス要件は、最小限の特権と Need to Know の原則に従って、職務機能に従って確立されている。		

要件とテスト手順		ガイダンス
		例えば、設定の責任と変更の承認の責任を別々の個人に割り当てることができます。 **定義** アクセスコントロールモデルの主な要素は以下の通りです。 • 保護すべきリソース（アクセスが必要なシステム／デバイス／データ）。 • リソースにアクセスする必要がある職務（例えば、システム管理者、コールセンターの担当者、店員）、および • 各職務が実行する必要のあるアクティビティ（例えば、read/write や query など）。 職能、リソース、職能ごとのアクティビティが定義されると、それに応じて個人にアクセス権が与えられます。 **例** 事業体が考慮できるアクセス制御モデルには、ロールベースアクセス制御（RBAC）および属性ベースアクセス制御（ABAC）が含まれる。特定の事業体が使用するアクセス制御モデルは、そのビジネスとアクセスの必要性に依存します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
7.2.2 特権ユーザを含むユーザには、以下に基づいてアクセスが割り当てられます。 • 職務分類と機能。 • 職責を果たすために必要な最小限の特権。	**7.2.2.a** ポリシーと手順を調べ、この要件で指定されたすべての要素に従ってユーザへのアクセス権を割り当てることを確認する。	**目的** 最小権限を割り当てることで、アプリケーションに関する十分な知識を持たないユーザが、誤ってアプリケーションの構成を変更したり、セキュリティ設定を変更したりすることを防ぐことができます。また、最小権限を付与することで、万が一、権限のない人がユーザ ID にアクセスした場合の被害範囲を最小限に抑えることができます。 **グッドプラクティス** アクセス権は、1 つまたは複数の機能への割り当てにより、ユーザに付与されます。アクセスは、特定のユーザ機能に応じて、業務に必要な最小限の範囲で割り当てられます。 特権的なアクセス権を割り当てる場合、個人が仕事を遂行するために必要な権限のみを割り当てることが重要です（「最小限の権限」）。例えば、データベース管理者やバックアップ管理者には、システム管理者全体と同じ権限を割り当てるべきではありません。 *(次ページに続く)*
	7.2.2.b 特権ユーザを含むユーザのアクセス設定を調査し、管理責任者にインタビューして、割り当てられた特権がこの要件で指定されているすべての要素に従っていることを確認する。	
	7.2.2.c アクセス権の割り当てに責任を持つ担当者にインタビューを行い、特権ユーザのアクセス権がこの要件で指定されたすべての要素に従って割り当てられていることを確認する。	

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 システムおよびデータへのアクセスは、関連するアクセス・ロールで定義された職務の遂行に必要なアクセスのみに制限されている。		ユーザ機能のニーズが定義されると（PCI DSS 要件 7.2.1 による）、すでに作成されているロールを使用して、職務分類と機能に応じたアクセスを個人に簡単に付与することができます。 これは、特権を持つアカウントに対して、その特権が必要なときだけアクセスを許可し、不要になったら直ちにそのアクセスを取り消す方法です。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
7.2.3 必要な権限は、任命された担当者によって承認される。	**7.2.3.a** ポリシーと手続きを調査し、任命された担当者がすべての権限を承認するプロセスを定義していることを確認する。	文書による承認（例えば、書面または電子的）により、アクセスおよび権限を持つ者が管理者に知られ、承認されていること、およびそのアクセスが職務上必要であることが保証されます。
カスタマイズアプローチの目的 適切な、文書化された承認がないユーザに対しては、アクセス権限を付与することはできない。	**7.2.3.b** ユーザ ID と割り当てられた権限を調べ、文書化された承認と比較し、以下のことを確認する。 • 割り当てられた権限に対して文書化された承認が存在する。 • 承認は任命された担当者によって行われている。 • 指定された権限が、個人に割り当てられた役割と一致している。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** アクセス権の定期的な見直しは、ユーザの職責変更、システム機能の変更、その他の変更後に残っている過剰なアクセス権を発見するのに役立ちます。過剰なアクセス権を適切な時期に失効させないと、悪意のあるユーザに不正に利用される可能性があります。 また、この見直しにより、解約したユーザのアカウントが削除されていること（解約時に見落としがあった場合）、アクセスが不要になった第三者のアカウントが削除されていることを確認する機会にもなります。 **グッドプラクティス** ユーザが新しい役割や部署に異動する場合、通常、以前の役割に関連する特権やアクセスはもはや必要ありません。不要になった権限や機能へのアクセスを継続すると、誤用やエラーのリスクが発生する可能性があります。したがって、職務が変更された場合、アクセスを再検証するプロセスにより、ユーザのアクセスが新しい職務に適切であることを確認することができます。 *(次ページに続く)*
7.2.4 サードパーティ／ベンダのアカウントを含む、すべてのユーザアカウントと関連するアクセス権を、以下のようにレビューする。 • 少なくとも半年に一度。 • ユーザアカウントおよびアクセス権が職務権限に基づき適切であることを確認する。 • 不適切なアクセスに対処する。 • 管理者は、アクセスが適切であることを確認する。	**7.2.4.a** ポリシーと手順を調査し、この要件で指定されているすべての要素に従って、サードパーティ／ベンダのアカウントを含むすべてのユーザアカウントと関連するアクセス権をレビューするプロセスを定義していることを確認する。	
カスタマイズアプローチの目的 アカウント権限の割り当てが正しいことを管理責任者が定期的に確認し、不適合は是正される。 *(次ページに続く)*	**7.2.4.b** 担当者にインタビューを行い、ユーザアカウントの定期的なレビューの文書化された結果を調べ、すべての結果がこの要件で指定されたすべての要素に準拠していることを確認する。	

要件とテスト手順		ガイダンス
適用に関する注意事項 この要件は、社員と第三者／ベンダーが使用するアカウント、第三者のクラウドサービスにアクセスするためのアカウントなど、すべてのユーザーアカウントと関連するアクセス権限に適用されます。 この要件は、ユーザアカウントおよび関連するアクセス権限に適用される。アプリケーションおよびシステムアカウントに対する制御については、要件 7.2.5 および 7.2.5.1、ならびに 8.6.1～8.6.3 を参照すること。 この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		企業は、アクセス権のレビューを行うための定期的かつ反復可能なプロセスを導入し、各自の職務権限に関連するデータへのアクセスを管理・監視する責任を負う「データオーナー」を任命し、ユーザのアクセスが最新かつ適切であることを確認することを検討することができます。例えば、ダイレクトマネージャーは毎月チームのアクセス権をレビューし、シニアマネージャーは四半期ごとにグループのアクセス権をレビューし、必要に応じてアクセス権の更新を行うことができます。これらのベストプラクティスの意図は、少なくとも 6 カ月に 1 回のレビューの実施を支援し、促進することです。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
7.2.5 すべてのアプリケーションおよびシステムアカウントと関連するアクセス権は、次のように割り当てられ、管理される。 • システムまたはアプリケーションの操作性に必要な最小限の権限に基づく。 • アクセスは、その使用を特に必要とするシステム、アプリケーション、またはプロセスに限定される。	**7.2.5.a** ポリシーと手順を調査し、この要件で指定されたすべての要素に従って、アプリケーションとシステムのアカウントおよび関連するアクセス権を管理および割り当てるためのプロセスを定義していることを確認する。	アプリケーションやシステムのアカウントに対して、適切なアクセスレベルを設定することが重要です。このようなアカウントが侵害された場合、悪意のあるユーザは、アプリケーションまたはシステムに付与されたものと同じアクセスレベルを取得することになります。したがって、システムおよびアプリケーションのアカウントには、ユーザアカウントと同じように制限されたアクセス権が付与されるようにすることが重要です。
カスタマイズアプローチの目的	**7.2.5.b** システムおよびアプリケーションのアカウントに関連する権限を調査し、担当者にインタビューして、アプリケーションおよびシステムのアカウントと関連するアクセス権限が、この要件で指定されているすべての要素に従って割り当てられ、管理されていることを確認する。	**グッドプラクティス**
アプリケーションおよびシステムのアカウントに付与されるアクセス権が、そのアプリケーションまたはシステムの運用に必要なアクセス権のみに限定されていること。		事業体は、これらのアプリケーションやシステムアカウントを設定する際に、事業体に該当する以下のような基本事項を設定することを検討するとよいでしょう。 • アカウントがドメイン管理者、ローカル管理者、ルートなどの特権グループのメンバーでないことを確認する。 • そのアカウントが使用できるコンピュータを制限する。 • 使用時間を制限する。 • VPN アクセスやリモートアクセスなどの追加設定を削除する。
適用に関する注意事項		
この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
7.2.5.1 アプリケーションおよびシステムアカウントによる全てのアクセスおよび関連するアクセス権限を以下のようにレビューする。 • 定期的に（要件 12.3.1 に規定された全ての要素に従って実施される、事業体の対象とするリスク分析で定義された頻度で）実施される。 • アプリケーション／システムへのアクセスが、実行される機能に対して適切な状態であり続けている。 • 不適切なアクセスには対処している。 • 管理責任者は、そのアクセスが適切な状態であり続けていることを認識する。	**7.2.5.1.a** ポリシーと手順を調べ、この要件で指定されたすべての要素に従って、すべてのアプリケーションとシステムのアカウントおよび関連するアクセス権をレビューするプロセスを定義していることを確認する。	アクセス権の定期的な見直しは、システムの機能変更など、アプリケーションやシステムの改変後に、過剰なアクセス権が残っていることを発見するのに役立ちます。過剰なアクセス権は、不要になった時点で削除しないと、悪意のあるユーザが不正アクセスに使用する可能性があります。
カスタマイズアプローチの目的	**7.2.5.1.b** アプリケーションおよびシステムのアカウント並びに関連するアクセス権の定期的なレビューの頻度について、事業体が対象とするリスク分析を調査し、リスク分析が要件 12.3.1 に規定されるすべての要素に従って実施されたことを確認する。	
アプリケーションやシステムのアカウント権限の割り当てが正しいかどうかを定期的に管理者が確認し、不適合は是正される。	**7.2.5.1.c** 担当者にインタビューを行い、システムおよびアプリケーションのアカウントと関連する特権の定期的なレビューの文書化された結果を調査し、この要件で指定されたすべての要素に従ってレビューが行われることを確認する。	
適用に関する注意事項		
この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** カード会員データ保存場所へのクエリアクセスの悪用は、データ漏洩のよくある原因です。このようなアクセスを管理者に制限することで、不正なユーザがこのようなアクセスを悪用するリスクを低減することができます。 **定義** 「プログラムによる方法」とは、エンドユーザ（管理業務のためにデータベースへの直接アクセスが必要な担当管理者を除く）がデータリポジトリに直接アクセスするのではなく、ユーザがテーブル内のデータに対して制御されたアクションを実行できるデータベースストアドプロシージャなどの手段を通じてアクセス権を付与することを意味します。 **グッドプラクティス** 代表的なユーザアクション は、データの移動、コピー、削除などです。また、アクセス権を付与する際には、必要な権限の範囲も考慮します。たとえば、データ要素、ファイル、テーブル、インデックス、ビュー、ストアドルーチンなど、特定のオブジェクトにアクセスを許可することができます。つまり、役割に基づき、各ユーザに割り当てられた特権のうち、職務を遂行するために必要なものだけが付与されるようにする必要があります。
7.2.6 保存されたカード会員データリポジトリへクエリを行うすべてのユーザアクセスは、以下のように制限される。 • アプリケーションまたはその他のプログラムによる方法で、ユーザの役割と最小特権に基づくアクセスおよび許可されたアクションを行う。 • 担当の管理者のみが、保存されたカード会員データ（CHD)のリポジトリに直接アクセスし、クエリすることができる。	**7.2.6.a** ポリシーと手順を調査し、担当者にインタビューして、この要件で指定されたすべての要素に 従って、保存されたカード会員データリポジトリへのクエリを行うユーザアクセス権を付与するためのプロセスが定義されていることを確認する。	
カスタマイズアプローチの目的 カード会員データのリポジトリに対するフィルタリングされていない（ad hoc）クエリの直接アクセスは、 許可された管理者によって実行されない限り、禁止されている。	**7.2.6.b** 保存されたカード会員データのリポジトリのクエリへの構成設定を調べ、それらがこの要件で指定されたすべての要素に準拠していることを確認する。	
適用に関する注意事項 この要件は、保存されたカード会員データリポジトリへのクエリを行うユーザアクセスのコントロールに適用される。 アプリケーションおよびシステムアカウントに対する制御については、要件 7.2.5 および 7.2.5.1、ならびに 8.6.1～8.6.3 を参照すること。		

要件とテスト手順		ガイダンス
7.3 システムコンポーネントおよびデータへの論理的なアクセスは、アクセス制御システムを介して管理される。		
定義されたアプローチの要件 **7.3.1** ユーザの知る必要性(Need to know)に基づいてアクセスを制限し、すべてのシステムコンポーネントをカバーするアクセス制御システム（複数可）がある。 **カスタマイズアプローチの目的** アクセス権および権限が、その目的のために意図されたメカニズムで管理されている。	**定義されたアプローチのテスト手順** **7.3.1** ベンダの文書およびシステム設定を調査し、各システムの構成要素について、ユーザの知る必要性(Need to know)に基づいてアクセスを制限するアクセス制御システムによってアクセスが管理され、すべてのシステム構成要素をカバーしていることを確認する。	**目的** ユーザの知る必要性(Need to know)に基づいてアクセスを制限するメカニズムがなければ、ユーザは知らないうちに カード会員データへのアクセスを許可される可能性があります。アクセス制御システムは、アクセスを制限し、権限を割り当てるプロセスを自動化します。
定義されたアプローチの要件 **7.3.2** アクセスコントロールシステムは、個人、アプリケーション、システムに割り当てられたアクセス許可を、職種と機能に基づいて強制するように設定されている。 **カスタマイズアプローチの目的** システム、アプリケーション、データに対する個人のアカウントアクセス権および権限は、グループメンバーからのみ継承される。	**定義されたアプローチのテスト手順** **7.3.2** ベンダの文書およびシステム設定を調査し、アクセス制御システムが、職務分類および機能に基づいて、個人、アプリケーションおよびシステムに割り当てられたアクセス許可を実施するように構成されていることを確認する。	**目的** アクセス制御システムにより特権的なアクセスを制限することで、個人、アプリケーション、およびシステムへの権限の割り当てに誤りが生じる機会を減らすことができます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** デフォルトの「すべて拒否」設定により、アクセスを許可する特別なルールが確立されていない限り、誰にもアクセスが許可されないことを保証します。 **グッドプラクティス** アクセス制御システムの中には、デフォルトで「すべてを許可する」設定になっているものがあり、その場合、特に拒否するルールを書かない限り、あるいは書くまではアクセスを許可してしまうので、デフォルトの設定を確認することが重要です。
7.3.3 アクセス制御システムはデフォルトで「すべて拒否」に設定されている。	**7.3.3** ベンダのドキュメントやシステムの設定を調べて、アクセス制御システムがデフォルトで「すべて拒否」に設定されていることを確認してください。	
カスタマイズアプローチの目的 明示的に許可された場合を除き、アクセス権および権限の使用を禁止する。		

要件 8：　ユーザの識別とシステムコンポーネントへのアクセスの認証

セクション
8.1 ユーザを識別し、システムコンポーネントへのアクセスを認証するためのプロセスおよびメカニズムが定義され、理解されている。
8.2 ユーザおよび管理者のユーザ識別および関連するアカウントは、アカウントのライフサイクルを通じて厳密に管理されている。
8.3 利用者および管理者の強力な認証が確立され、管理されている。
8.4 カード会員データ環境（CDE)へのアクセスを保護するために、多要素認証（MFA）を導入している。
8.5 多要素認証（MFA）システムが、悪用を防ぐために設定されている。
8.6 アプリケーションおよびシステムアカウントの使用および関連する認証要素は厳重に管理されている。

概要

ユーザの識別と認証の 2 つの基本原則は、1）コンピュータ・システム上の個人またはプロセスの識別を確立すること、2）識別に関連するユーザがそのユーザが主張する人物であることを証明または検証することです。

コンピュータシステム上の個人またはプロセスの識別は、ユーザ ID、システム ID、アプリケーション ID などの識別子を通じて、個人またはプロセスに ID を関連付けることによって行われます。これらの ID（「アカウント」とも呼ばれる）は、基本的に、あるユーザまたはプロセスを他のユーザまたはプロセスと区別するために、各個人またはプロセスに固有の識別を割り当てることによって、個人またはプロセスのアイデンティティを確立します。各ユーザまたはプロセスが一意に識別できれば、その ID で実行されたアクションに対する説明責任が確保されます。そのような説明責任がある場合、実行されたアクションは、既知の承認されたユーザおよびプロセスに対して追跡することができます。

I ユーザの識別を証明または検証するために使用される要素は、認証要素として知られています。認証要素は、1）パスワードやパスフレーズなどの知識情報、2）トークン・デバイスやスマート・カードなどの所持情報、3）生体認証などの生体情報です。

ID と認証要素を合わせて認証クレデンシャルと考え、ユーザ、アプリケーション、システム、またはサービスアカウントに関連するアクセス権や権限に使用されます。

(次ページに続く)

ID および認証に関するこれらの要件は、決済エコシステムをサポートするために、業界で受け入れられたセキュリティ原則およびベストプラクティスに基づいています。*NIST Special Publication800-63『Digital Identity Guidelines』* は、デジタル ID および 認証要素 のための許容可能なフレームワークに関する追加情報を提供します。*『Digital Identity Guidelines』*は、米国連邦政府機関を対象としており、その全体を参照する必要があることに留意することが重要です。このガイドラインで定義された概念やアプローチの多くは、独立したパラメータとしてではなく、互いに連動することが期待されています。

注：*要件に特に記載がない限り、これらの要件は、個々の要件で特に呼び出されていない限り、****すべてのシステムコンポーネントのすべてのアカウント****に適用されます。例えば以下を含みますが、これらに限定されません。*

- *販売時点情報管理（POS）アカウント*
- *管理機能を有するアカウント*
- *システムおよびアプリケーションのアカウント*
- *カード会員データを表示またはアクセスするため、またはカード会員データを含むシステムにアクセスするため に使用されるすべてのアカウント。*

これには、従業員、請負業者、コンサルタント、社内外のベンダ、およびその他のサードパーティ（サポートまたはメンテナンスサービスを提供するためなど）が使用するアカウントが含まれます。

一部の要件は、単一のトランザクションを促進するために一度に 1 つのカード番号のみにアクセス するユーザアカウント（POS 端末のレジ係が使用する ID など）には適用されないよう意図されています。適用されない項目がある場合は、特定の要件に直接記載されます。

これらの要件は、消費者（カード会員）が使用するアカウントには適用されません。

PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
8.1 ユーザを識別し、システムコンポーネントへのアクセスを認証するためのプロセスおよびメカニズムが定義され、理解されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.1.1 要件 8 で特定されたすべてのセキュリティポリシーと運用手順がある。 • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に知られている。	**8.1.1** 要件 8 で特定されたセキュリティポリシーと運用手順が、この要件で規定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューする。	要件 8.1.1 は、要件 8 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 8 で呼び出された特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及していることを確認することも同様に重要です。 **グッドプラクティス** プロセス、技術、事業目的の変化に対応するため、必要に応じてポリシーや手順を更新することが重要です。そのため、定期的な更新だけでなく、変更が発生したらできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、事業体のセキュリティの目的および原則を定義するものです。運用手順は、アクティビティの実行方法を記述し、一貫した方法で、ポリシーの目的に従って望ましい結果を達成するために従う統制、方法、プロセスを定義します。
カスタマイズアプローチの目的		
要件 8 内のアクティビティを満たすために期待されること、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべてのサポートアクティビティが繰り返し可能であり、一貫して適用され、経営者の意図に適合している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要なアクティビティが行われない可能性があります。 **グッドプラクティス** 役割と責任は、ポリシーと手順の中で文書化されるか、または別の文書で管理されるかもしれません。 役割と責任を伝える一環として、事業体は担当者が与えられた役割と責任を受け入れ、理解したことの確認を検討することができます。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担マトリックス（RACI マトリックスとも呼ばれる）があります。
8.1.2 要件 8 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**8.1.2.a** 文書を調査し、要件 8 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	8.1.2.b 要件 8 の活動の実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 8 のすべての活動を実施するための日常的な責任が割り当てられている。担当者は、これらの要件の成功、継続的な運用に責任を負う。		

要件とテスト手順		ガイダンス
8.2 ユーザと管理者の識別と関連するアカウントは、アカウントのライフサイクルを通じて厳密に管理されている。		
定義されたアプローチの要件 **8.2.1** すべてのユーザには、システムコンポーネントまたはカード会員データへのアクセスが許可される前に、一意の ID が割り当てられる。 **カスタマイズアプローチの目的** すべての利用者のすべての行為が個人に帰属する。 **適用に関する注意事項** この要件は、トランザクションを 1 件処理するために一度に 1 つのカード番号のみにアクセスできる POS 端末内のユーザアカウント（POS 端末のレジ担当者が使用する ID など）に適用することは意図していない。	**定義されたアプローチのテスト手順** **8.2.1.a** 担当者にインタビューし、すべてのユーザがシステムコンポーネントおよびカード会員データにアクセスするために一意の ID を割り当てられていることを確認する。 **8.2.1.b** 監査ログおよびその他の証拠を調査し、システムコンポーネントおよびカード会員データへのアクセス が一意に識別され、個人に関連付けられることを検証する。	**目的** コンピュータ・システム上で行われたアクションを個人まで追跡できることは、説明責任とトレーサビリティを確立し、効果的なアクセス制御を確立するための基本です。 複数の従業員に対して 1 つの ID を使用するのではなく、各ユーザが一意に識別されるようにすることで、事業体は個々の行動に対する責任を維持し、従業員ごとに監査ログに効果的に記録することができます。さらに、誤用や悪意が生じた場合の問題解決や封じ込めに役立てることができます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.2.2 グループアカウント、共有アカウント、汎用アカウント、またはその他の共有された認証情報は、例外的に必要な場合のみ使用し、以下のように管理される。 • 例外的に必要な場合を除き、アカウントの利用を禁止する。 • 使用は例外的な状況に必要な時間に制限される。 • 使用を正当化するビジネス上の理由が文書化されている。 • 使用は、経営陣によって明示的に承認される。 • アカウントへのアクセスが許可される前に、個々のユーザの身元が確認される。 • 実行されたすべてのアクションが、個々のユーザに起因するものである。	**8.2.2.a** システム・コンポーネントのユーザ・アカウント・リストおよび該当する文書を調査し、共有された認証情報が必要な場合にのみ、例外的に使用され、この要件で指定されたすべての要素に従って管理されていることを確認する。 **8.2.2.b** 認証ポリシーおよび手順を調べて、共有された認証情報が必要なときにのみ例外的に使用され、この要件で指定されたすべての要素に従って管理されるように、プロセスが定義されていることを確認する。 **8.2.2.c** システム管理者にインタビューを行い、共有された認証情報が必要なときのみ、例外的に使用され、この要件で指定されたすべての要素に従って管理されていることを確認する。	グループアカウント、共有アカウント、汎用（またはデフォルト）アカウントは、通常、ソフトウェアやオペレーティングシステムと一緒に提供されます-例えば、ルートまたは管理者のような特定の機能に関連する特権を持ちます。 複数のユーザが同じ認証情報（例えば、ユーザアカウントとパスワード）を共有する場合、システムアクセスやアクティビティから個人を特定することが不可能になります。その結果、ある行動は、ユーザ ID および関連する認証要素を知っているグループ内の誰でも実行できるため、事業体が個人の行動に対する説明責任を割り当てたり、効果的なログを取ることができなくなります。 アカウントで実行されたアクションに個人を関連付ける機能は、誰がアクションを実行したか、どんなアクションが実行されたか、そのアクションがいつ発生したかに関する個人の説明責任とトレーサビリティを提供するために不可欠です。 *(次ページに続く)*
カスタマイズアプローチの目的		
汎用 ID、システム ID、共有 ID を持つユーザが行ったすべてのアクションが、個人に帰属すること。		

要件とテスト手順		ガイダンス
適用に関する注意事項 この要件は、トランザクションを 1 件処理するために一度に 1 つのカード番号のみにアクセスできる POS 端末内のユーザアカウント（POS 端末のレジ担当者が使用する ID など）に適用することは意図していない。		**グッドプラクティス** 何らかの理由で共有アカウントを使用する場合、個々の説明責任とトレーサビリティを維持するために、強力な管理統制を確立する必要があります。 **例** ツールや技術によって、この種のアカウントの管理とセキュリティの両方を容易にし、アカウントへのアクセスが許可される前に個々のユーザの身元を確認することができる。事業体は、パスワード保管庫や、*sudo* コマンドのようなシステムで管理される制御を検討することができます。 例外的な状況の例としては、他のすべての認証方法が失敗し、緊急の使用のために共有アカウントが必要な場合です。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.2.3 ***サービスプロバイダのみに対する追加要件:顧客環境へ***リモートアクセスするサービスプロバイダは、顧客環境ごとに一意の認証要素を使用する。	**8.2.3** ***サービスプロバイダ評価のみの追加テスト手順：***顧客環境へのリモートアクセスを行うサービスプロバイダが、各顧客環境へのリモートアクセスに固有の認証要素を使用していることを確認するために、認証ポリシーと手順を調べ、担当者にインタビューを行う。	顧客環境にリモートアクセスするサービスプロバイダは、通常、POS POI システムのサポートやその他のリモートサービスを提供するために、このアクセスを使用します。 サービスプロバイダが複数の顧客にアクセスするために同じ認証要素を使用する場合、攻撃者がその 1 つの要素を侵害すると、サービスプロバイダのすべての顧客に簡単に侵入される可能性があります。 *(次ページに続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 ある顧客に使用されたサービスプロバイダの資格情報は、他の顧客には使用できない。 **適用に関する注意事項** この要件は、複数の顧客環境がホストされている、独自の共有サービス環境にアクセスするサービスプロバイダへの適用を意図したものではない。 サービスプロバイダの従業員が顧客環境にリモートアクセスするために共有された認証要素を使用する場合、これらの要素は顧客ごとに一意でなければならず、要件 8.2.2 に従って管理される必要がある。 この要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用される。		犯罪者はこれを知っており、単一の認証要素で多くの加盟店にリモートアクセスできる共有された認証要素を求めて、意図的にサービスプロバイダをターゲットにしています。 **例** 各接続に一意の資格情報を提供する多要素メカニズム（使い捨てパスワードなど）のような技術も、この要件の意図を満たすことができる。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.2.4 ユーザ ID、認証要素、その他の識別子オブジェクトの追加、削除、変更は以下のように管理される。 • 適切な承認を得ていること。 • 文書化された承認に定められた権限のみで実施されていること。	**8.2.4** アカウントのライフサイクル（追加、変更、削除）のさまざまな段階にわたって文書化された権限を調査し、システム設定を調べて、この要件で指定されたすべての要素に従って活動が管理されていることを確認します。	ユーザ ID のライフサイクル（追加、削除、変更）を管理し、許可されたアカウントのみが機能を実行でき、アクションは監査可能で、権限は必要なものだけに制限されることが必須です。 攻撃者はしばしば、既存のアカウントを侵害し、そのアカウントの権限を昇格させて不正な行為を行ったり、バックグラウンドで活動を継続するために新しい ID を作成することがあります。通常の変更プロセス以外で、あるいは相応の権限を持たずにユーザアカウントが作成・変更された場合、それを検知して対応することが不可欠です。
カスタマイズアプローチの目的		**目的**
ユーザ ID および認証要素のライフサイクルイベントは、適切な承認が必ず伴う。		従業員または第三者／ベンダが退職した後も、そのユーザアカウントを介してネットワークにアクセスできる場合、元従業員または旧アカウントや未使用アカウントを悪用する悪意のあるユーザによって、カード会員データに不必要または悪意を持ってアクセスされる可能性があります。
適用に関する注意事項		
この要件は、従業員、契約社員、コンサルタント、派遣社員、第三者ベンダを含む、すべてのユーザアカウントに適用される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
8.2.5 契約終了したユーザのアクセスは直ちに取り消される。	**8.2.5.a** 契約終了したユーザの情報のソースを調べ、ローカルアクセスとリモートアクセスの両方について、現在のユーザアクセスリストを確認し、終了したユーザ ID が無効化されているか、アクセスリストから削除されていることを確認する。	
	8.2.5.b 担当者にインタビューを行い、終了したユーザーについて、スマートカード、トークンなどのすべての物理的な認証要素が返却または無効化されていることを確認する。	
カスタマイズアプローチの目的		
契約終了したユーザのアカウントは使用できない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **8.2.6** 非アクティブなユーザアカウントは、非アクティブ化された日から 90 日以内に削除または無効化される。 **カスタマイズアプローチの目的** 非アクティブなユーザアカウントは使用できない。	**定義されたアプローチのテスト手順** **8.2.6** ユーザーアカウントと最終ログオン情報を調査し、担当者にインタビューして、非アクティブなユーザーアカウントが 90 日以内に削除または無効化されていることを確認する。	**目的** 普段使っていないアカウントは、パスワードの変更などに気づかれにくいため、攻撃対象になりやすい。そのため、これらのアカウントは、カード会員データにアクセスするために、より容易に悪用される可能性があります。 **グッドプラクティス** 長期休暇など、長期間アカウントが使用されないことが合理的に予想される場合は、90 日間待たずに、休暇開始と同時にアカウントを無効化する必要があります。
定義されたアプローチの要件 **8.2.7** リモートアクセスによりシステムコンポーネントにアクセス、サポート、または保守のために第三者が使用するアカウントは、次のように管理される。 • 必要な時間帯のみ有効化し、使用しないときは無効化する。 • 予期せぬ事態が発生しないよう監視する。	**定義されたアプローチのテスト手順** **8.2.7** 担当者にインタビューし、アカウント管理のための文書を調査し、第三者がリモートアクセスのために使用するアカウントがこの要件で指定されたすべての要素に従って管理されていることを確認するために証拠を調査する。	**目的** 第三者がサポートを必要とする場合に備え、24 時間 365 日、事業体のシステムやネットワークにアクセスできるようにすることは、不正アクセスの可能性を高めます。このアクセスは、第三者環境における未許可のユーザ、または悪意のある個人が、事業体のネットワークへの常時利用可能な外部エントリーポイントを使用することになりかねません。第三者が 24 時間 365 日アクセスする必要がある場合は、文書化し、正当化し、監視し、特定のサービス理由と関連付ける必要があります。 *(次ページに続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 特別に許可され、管理者によって使用が監督されている場合を除き、第三者のリモートアクセスを使用することはできない。		**グッドプラクティス** 必要な時間だけアクセスできるようにし、不要になったらすぐに無効にすることで、接続の悪用を防ぐことができます。また、第三者との契約に基づき、アクセスの開始日と停止日を設定することを検討します。 第三者によるアクセスを監視することで、第三者が必要なシステムのみにアクセスし、承認された時間帯にのみアクセスしていることを確認することができます。第三者のアカウントを使用した異常な活動は、追跡調査し解決する必要があります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
8.2.8 ユーザセッションが 15 分以上アイドル状態の場合、端末またはセッションを再度アクティブにするために再認証が必要です。	**8.2.8** システム構成設定を調査し、ユーザセッションのシステム／セッションアイドルタイムアウト機能が 15 分以下に設定されていることを確認する。	**目的** システムコンポーネントまたはカード会員データにアクセスできるオープンなマシンからユーザが離れるとき、ユーザ不在の間に他のユーザによってマシンが使用され、不正なアカウントアクセスや誤用につながるリスクがあります。 **グッドプラクティス** 再認証は、そのマシン上で実行されているすべてのセッションを保護するためにシステムレベルで、またはアプリケーションレベルで適用することができます。 また、時間の経過とともに無人セッションのアクセスをさらに制限するために、制御を連続的にステージングすることを検討することもできます。たとえば、15 分後にスクリーンセーバーを起動し、1 時間後にユーザをログオフさせるなどです。 ただし、タイムアウト制御は、アクセスや露出のリスクと、ユーザへの影響およびアクセスの目的とのバランスをとる必要があります。 無人コンピュータからプログラムを実行する必要がある場合、ユーザはコンピュータにログインしてプログラムを開始し、コンピュータが無人である間、他の誰もユーザのログインを使用できないようにコンピュータを「ロック」することが可能でです。 *(次ページに続く)*
カスタマイズアプローチの目的		
ユーザセッションは、許可されたユーザ以外には使用できない。		
適用に関する注意事項		
この要件は、1 つの取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウント（POS 端末のレジ係が使用する ID など）に適用することを意図していない。 この要件は、コンソール／PC が無人である間に正当な活動が行われることを防ぐためのものではない。		

要件とテスト手順		ガイダンス
		例 この要件を満たす 1 つの方法は、コンソールが 15 分間アイドル状態のときに自動スクリーンセーバーが起動するように設定し、ログインユーザがパスワードを入力して画面のロックを解除することを要求することです。

要件とテスト手順		ガイダンス
8.3 利用者および管理者の強力な認証が確立され、管理されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.3.1 ユーザと管理者のシステムコンポーネントへのすべてのユーザアクセスは、以下の認証要素のうち少なくとも 1 つを経由して認証されます。 • パスワードやパスフレーズなど、ユーザが知っていること • トークン・デバイスやスマート・カードなど、ユーザが所有しているもの • バイオメトリクス要素など、ユーザ自身を示すもの	**8.3.1.a** システム・コンポーネントへのユーザ・アクセスが、この要件で指定された少なくとも 1 つの認証要素を介して認証されていることを確認するために使用される認証要素を説明する文書を調べる。	一意の ID に加えて認証要素を使用する場合、攻撃者は一意の ID を持ち、関連する認証要素を侵害する必要があるため、ユーザ ID が侵害されないように保護するのに役立ちます。
カスタマイズアプローチの目的	**8.3.1.b** 各タイプのシステムコンポーネントで使用される各認証要素について、認証を観察し、認証が文書化された認証要素で一貫して機能することを確認する。	**グッドプラクティス**
アカウントは、ユーザ ID と認証要素の組み合わせ以外ではアクセスできない。		悪意のある個人がシステムを侵害する一般的な方法は、弱い、あるいは存在しない認証要素（例えば、パスワード／パスフレーズ）を悪用することです。強力な認証要素を要求することは、この攻撃から保護するのに役立ちます。
適用に関する注意事項		**その他の情報**
この要件は、1 つの取引を促進するために一度に 1 つのカード番号にのみアクセスできる POS 端末のユーザアカウント（POS 端末のレジ担当者が使用する ID など）に適用することは意図していない。 この要件は、多要素認証（MFA）要件に取って代わるものではないが、MFA 要件の適用範囲外である対象システムにも適用される。 デジタル証明書は、特定のユーザにとって一意である場合、所持情報の有効なオプションである。		トークン、スマートカード、バイオメトリクスを認証要素として使用する場合の詳細については、*fidoalliance.org* を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **8.3.2** 強力な暗号を使用して、すべてのシステムコンポーネントで送信中および保存中のすべての認証要素を読み取り不能にする。	**定義されたアプローチのテスト手順** **8.3.2.a** ベンダのドキュメントやシステム構成設定を調べ、認証要素が送信および保存時に強力な暗号で読み取り不能にされていることを確認する。 **8.3.2.b** 認証要素のリポジトリを調査し、保管中に読み取り不可能であることを確認する。 **8.3.2.c** データ伝送を検査し、認証要素が伝送中に読み取り不能であることを確認する。	**目的** ネットワーク機器とアプリケーションは、暗号化されていない読み取り可能な認証要素（パスワードやパスフレーズなど）をネットワーク経由で送信したり、これらの値を暗号化せずに保存したりすることが知られています。その結果、悪意のある個人が「スニッファー（sniffer）」を使って送信中の情報を簡単に傍受したり、暗号化されていない認証要素が保存されているファイルに直接アクセスして、このデータを使って不正なアクセスを行うことができます。
カスタマイズアプローチの目的 通信の傍受または保存されたデータから、平文の認証要素を取得、派生、または再利用することはできない。		
定義されたアプローチの要件 **8.3.3** 認証要素を変更する前に、利用者の身元が確認される。	**定義されたアプローチのテスト手順** **8.3.3** 認証要素の変更手順を調査し、セキュリティ担当者を観察して、ユーザが認証要素の変更を要求した場合、認証要素が変更される前にユーザの身元が確認されることを確認する。	**目的** 悪意のある人は、「ソーシャル・エンジニアリング」の手法を用いて、システムのユーザになりすまし、例えば、ヘルプデスクに電話をかけて正当なユーザを装い、認証要素を変更させ、有効なユーザ ID を使用できるようにします。 このような攻撃が成功する確率を減らすために、ユーザの本人確認が必要です。 *(次ページに続く)*
カスタマイズアプローチの目的 権限のない個人が、権限のあるユーザの身元を偽ってシステムにアクセスすることはできない。		

要件とテスト手順		ガイダンス
		グッドプラクティス ユーザの身元を確認する必要がある認証要素の変更には、パスワードのリセット、新しいハードウェアまたはソフトウェア・トークンのプロビジョニング、新しい鍵の生成などが含まれますが、これらに限定されるものではありません。 **例** ユーザの身元を確認する方法としては、秘密の質問／回答、知識ベースの情報、既知の確立された電話番号にユーザをコールバックする方法などがあります。
定義されたアプローチの要件 **8.3.4** 無効な認証の試行は、以下の方法で制限される。 • 10 回以下の試行回数でユーザ ID をロックアウトする。 • ロックアウトの時間は最低 30 分、または本人確認ができるまでとする。 **カスタマイズアプローチの目的** 認証要素は、総当たりのオンライン攻撃では推測できない。	**定義されたアプローチのテスト手順** **8.3.4.a** システム構成設定を調査し、認証パラメータが、無効なログオン試行回数 10 回以下でユーザアカウントをロックアウトするよう設定されていることを確認する。 **8.3.4.b** システム構成設定を調査し、ユーザアカウントが一度ロックアウトされると、最低 30 分間またはユーザの身元が確認されるまでロックされたままにすることを要求するパスワードパラメータが設定されていることを確認する。	**目的** アカウントロックアウトの仕組みがないと、攻撃者は手動または自動ツール（パスワード解読ツールなど）を使ってパスワードを推測し続け、成功するとユーザのアカウントにアクセスできるようになります。 誰かが継続的にパスワードを推測しようとしたためにアカウントがロックアウトされた場合、ロックされたアカウントの再アクティブ化を遅らせるためのコントロールは、アカウントが再アクティブ化されるまで最低 30 分間停止しなければならないので、悪意のある個人がパスワードを推測するのを阻止することができます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
適用に関する注意事項 この要件は、1 つの取引を促進するために一度に 1 つのカード番号にのみアクセスできる POS 端末のユーザアカウント（POS 端末のレジ担当者が使用する ID など）に適用することは意図していない。		**グッドプラクティス** ロックされたアカウントを再有効化する前に、ユーザの身元を確認する必要があります。例えば、管理者またはヘルプデスク担当者が、実際のアカウント所有者が再有効化を要求していることを確認することができますし、またはアカウント所有者が自分の身元を確認するために使用するパスワードリセットのセルフサービスのメカニズムを利用することもできます。
定義されたアプローチの要件 **8.3.5** 要件 8.3.1 を満たすためにパスワード／パスフレーズを認証要素として使用する場合、次のようにユーザごとに設定／解除する。 • 初回使用時およびリセット時にはユニークな値を設定する。 • 初回使用後直ちに強制的に変更する。	**定義されたアプローチのテスト手順** **8.3.5** パスワード／パスフレーズ（要件 8.3.1 を満たす認証要素として使用される場合）の設定とリセットの手順を調べ、セキュリティ担当者を観察して、パスワード／パスフレーズがこの要件で指定されるすべての要素に従って設定およびリセットされていることを確認する。	**目的** 新規ユーザに対して毎回同じパスワード／パスフレーズを使用すると、内部ユーザ、元社員、悪意のある個人がその値を知っているか容易に発見し、正規ユーザがパスワードを使用しようとする前に、その値を使用してアカウントにアクセスすることができる可能性があります。
カスタマイズアプローチの目的 ユーザに割り当てられた初期または再設定のパスワード／パスフレーズは、権限のないユーザには使用できない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.3.6 要件 8.3.1 を満たすためにパスワード／パスフレーズを認証要素として使用する場合、以下の最小レベルの複雑さを満たすこと。 • 12 文字以上（またはシステムが 12 文字に対応していない場合は、8 文字以上）であること。 • 数字とアルファベットの両方が含まれていること。	**8.3.6** システム構成設定を調査し、ユーザパスワード／パスフレーズの複雑さパラメータが、この要件で指定されたすべての要素に従って設定されていることを確認する。	悪意のある者は、しばしば弱い、変更されない、または存在しないパスワードでアカウントを最初に見つけようとするので、強いパスワード／パスフレーズは、ネットワークへの最初の防衛線かもしれません。パスワードが短かったり、簡単に推測できる場合、悪意のある個人がこれらの弱いアカウントを見つけ、有効なユーザ ID を装ってネットワークを侵害することは比較的容易です。 **グッドプラクティス** パスワード／パスフレーズの強度は、パスワード／パスフレーズの複雑さ、長さ、およびランダム性に依存します。パスワード／パスフレーズは、攻撃者がその値を推測したり、発見したりすることが現実的でないように、十分に複雑であるべきです。事業者は、この要件で概説された最低基準に加え、特殊文字や大文字と小文字の使用を義務付けることで、複雑さを増すことを検討することができます。複雑さを増すと、ハッシュ化されたパスワード／パスフレーズに対するオフラインでの総当たり攻撃に必要な時間が長くなります。 推測攻撃に対するパスワードの耐性を高めるもう一つの方法は、提案されたパスワード／パスフレ *(次ページに続く)*
カスタマイズアプローチの目的		
パスワード／パスフレーズは、オンラインまたはオフラインの総当たり攻撃で推定することができない。		
適用に関する注意事項		
この要件は、以下に適用することを意図していない。 • 一度に 1 つのカード番号にのみアクセスし、1 つの取引を促進する POS 端末のユーザアカウント（POS 端末のキャッシャーが使用する ID など） • 8.6 項の要件によって管理されるアプリケーションまたはシステムアカウント *(次ページに続く)*		

要件とテスト手順		ガイダンス
この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。 2025 年 3 月 31 日までは、PCI DSS v3.2.1 要件 8.2.3 に従って、パスワードは最低 7 文字である必要がある。		ーズをバッドパスワードリスト(bad password list)と比較し、リスト上で見つかったパスワードの代わりにユーザに新しいパスワードを提供させることです。
定義されたアプローチの要件 **8.3.7** 個人が過去に使用した 4 つのパスワード／パスフレーズのいずれかと同じ新しいパスワード／パスフレーズを使用することは許可しない。 **カスタマイズアプローチの目的** 少なくとも 12 カ月間、以前に使用したパスワードでアカウントにアクセスすることはできない。 **適用に関する注意事項** この要件は、1 つの取引を促進するために一度に 1 つのカード番号にのみアクセスできる POS 端末のユーザアカウント（POS 端末のレジ担当者が使用する ID など）に適用することは意図していない。	**定義されたアプローチのテスト手順** **8.3.7** システム構成設定を調査し、新しいパスワード／パスフレーズが以前に使用された 4 つのパスワード／パスフレーズと同じであってはならないことを要求するようにパスワードパラメータが設定されていることを確認する。	**目的** パスワードの履歴が管理されていないと、以前のパスワードが何度も再利用されるため、パスワード変更の有効性が低下します。パスワードの再利用を一定期間禁止することで、推測や総当たりされたパスワードが将来的に再利用される可能性を低減することができます。 パスワードやパスフレーズは、漏洩の疑いや有効期限を超えたために以前に変更されたことがある可能性があります。これらいずれの場合も、以前に使用されたパスワードを再利用してはなりません。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.3.8 認証の方針と手順が文書化され、以下を含む全ユーザに伝達されている。 • 強力な認証要素の選択に関するガイダンス • ユーザがどのように認証要素を保護すべきかのガイダンス • 以前に使用したパスワード／パスフレーズを再利用しないようにするための指示 • パスワード／パスフレーズが漏洩した疑いがある場合、または漏洩したことが判明した場合、パスワード／パスフレーズを変更すること、およびそのインシデントを報告する方法についての指示	**8.3.8.a** 手順を調べ、担当者にインタビューし、認証ポリシーと手順が全ユーザに配布されていることを確認する。	認証の方針と手順をすべてのユーザに伝えることで、ユーザが方針を理解し、それを順守することができます。
	8.3.8.b 利用者に配布された認証ポリシーおよび手順をレビューし、それらがこの要件で指定された要素を含んでいることを確認する。	**グッドプラクティス** 強力なパスワードの選択に関するガイダンスには、辞書的な単語や、ユーザ ID、家族の名前、生年月日などのユーザに関する情報を含まない、推測しにくいパスワードを担当者が選択できるようにするための提案を含めることができます。 認証要素を保護するためのガイダンスには、パスワードを書き留めない、安全でないファイルに保存しない、パスワードを悪用しようとする悪意のある人物に注意する（例えば、従業員に電話をかけてきて、「問題のトラブルシューティング」ができるようにパスワードを聞き出すなど）ことが含まれる場合があります。 また、パスワードがパスワードポリシーに適合していることを確認するプロセスを導入することもできます。例えば、選択したパスワードを許容できないパスワードのリストと比較し、リスト上のパスワードと一致するものは、ユーザに新しいパスワードを選択させるなどの方法があります。 *(次ページに続く)*
カスタマイズアプローチの目的		
ユーザは、認証要素の正しい使用に関する知識を有し、必要に応じて支援やガイダンスにアクセスすることができる。		

要件とテスト手順		ガイダンス
		パスワードが安全でなくなった可能性がある場合、パスワードを変更するようユーザに指示することで、悪意のあるユーザが正当なパスワードを使って不正アクセスすることを防ぐことができます。
定義されたアプローチの要件 **8.3.9** パスワード／パスフレーズが、ユーザアクセスのための唯一の認証要素として使用される場合（すなわち、一要素認証の実装において）、以下のいずれかが行われる。 • パスワード／パスフレーズが少なくとも 90 日に 1 回変更されていること。 **または** • アカウントのセキュリティ状態を動的に分析し、それに応じてリソースへのリアルタイムアクセスを自動的に決定します。 **カスタマイズアプローチの目的** 漏洩が発見されなかったパスワード／パスフレーズは、無期限に使用できない。	**定義されたアプローチのテスト手順** **8.3.9** ユーザアクセスのための唯一の認証要素としてパスワード／パスフレーズを使用している場合、システム構成設定を検査し、パスワード／パスフレーズがこの要件で指定されている要素のいずれかに従って管理されていることを確認する。	**目的** カード会員データ環境（CDE）に含まれない対象システムコンポーネントへのアクセスは、パスワード／パスフレーズ、トークン装置またはスマートカード、または生体属性などの単一の認証要素を使用して提供される場合があります。パスワード／パスフレーズがこのようなアクセスのための唯一の認証要素として採用される場合、パスワード／パスフレーズの完全性を保護するための追加のコントロールが必要とされる。 **グッドプラクティス** パスワード／パスフレーズを変更せずに長期間有効にしておくと、悪意のある人物にパスワード／パスフレーズを破られる時間が長くなる。定期的にパスワードを変更することで、悪意のある個人がパスワード／パスフレーズを解読する時間を短縮し、漏洩

要件とテスト手順		ガイダンス
適用性の注記 この要件は、カード会員データ環境（CDE）に含まれない対象システムコンポーネントには MFA 要件が適用されないため、対象システムコンポーネントに適用される。この要件は、1 回の取引を促進するために一度に 1 つのカード番号のみにアクセスできる POS 端末のユーザアカウント（POS 端末のレジ係が使用する ID など）に適用することを意図していない。 この要件は、サービスプロバイダの顧客アカウントには適用されませんが、サービスプロバイダの担当者のアカウントには適用されます。		したパスワードを使用する時間を短縮することができます。 パスワード／パスフレーズを唯一の認証要素として使用することは、漏洩した場合の単一障害点となる。したがって、これらの実装では、漏洩したパスワード／パスフレーズを介して悪意のある活動が発生する時間を最小限に抑えるための制御が必要です。 アカウントのセキュリティ状態を動的に分析することは、漏洩した可能性のある認証情報をより迅速に検知し、対処することを可能にするもう一つの選択肢です。このような分析では、デバイスの完全性、場所、アクセス時間、およびアクセスされたリソースを含む多くのデータポイントを使用して、要求されたリソースへのアクセスをアカウントが許可されるかどうかをリアルタイムで判断することができる。このようにして、認証情報の漏洩が疑われる場合、アクセスを拒否し、アカウントをブロックすることができる。 **その他の情報** リソースへのユーザアクセスを管理するための動的分析の使用に関する情報は、NIST SP 800-207 ゼロトラストアーキテクチャを参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.3.10 ***サービスプロバイダのみに対する追加要件:*** 顧客ユーザがカード会員データにアクセスするための唯一の認証要素としてパスワード／パスフレーズを使用する場合（すなわち、1 要素認証の実装において）、顧客ユーザに対して以下を含むガイダンスが提供される。 • 顧客に対して、ユーザパスワード／パスフレーズを定期的に変更するようガイダンスする。 • パスワード／パスフレーズをいつ、どのような状況で変更するかについてのガイダンス。	**8.3.10** ***サービスプロバイダ評価のみの追加試験手順：<2> サービスプロバイダ評価のみの追加試験手順：***顧客ユーザがカード会員データにアクセスするための唯一の認証要素としてパスワード／パスフ レーズを使用する場合、顧客ユーザに提供されるガイダンスを検証し、ガイダンスにこの要件で指定 されたすべての要素が含まれていることを検証する。	パスワード／パスフレーズを唯一の認証要素として使用すると、漏洩した場合に単一障害点となる。したがって、これらの実装では、漏洩したパスワード／パスフレーズを介して悪意ある活動が発生する時間を最小限に抑えるための制御が必要である。 **グッドプラクティス** パスワード／パスフレーズを変更せずに長期間有効な場合、悪意のある人物にパスワード／パスフレーズを解読される時間が長くなります。定期的にパスワードを変更することで、悪意のある個人がパスワード／パスフレーズを解読する時間を短縮し、漏洩したパスワードを使用する時間を短縮することができます。
カスタマイズアプローチの目的 サービス提供者の顧客のパスワード／パスフレーズを無期限に使用できない。		
適用性の注記 この要件は、自身のペイメントカード情報にアクセスする消費者ユーザのアカウントには適用されません。 この要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用されます。 サービスプロバイダに対するこの要件は、8.3.10.1 が有効になると、要件 8.3.10.1 によって置き換えられる予定である。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.3.10.1 ***サービスプロバイダのみに対する追加要件：*** パスワード／パスフレーズを顧客ユーザアクセスの唯一の認証要素として使用する場合（すなわち、1 要素認証の実装において）、以下のいずれかを行う。 • パスワード／パスフレーズが少なくとも 90 日に 1 回変更されていること。 **または** • アカウントのセキュリティ状態を動的に分析し、それに応じてリソースへのリアルタイムアクセスを自動的に決定します。	**8.3.10.1** ***サービスプロバイダ評価のみの追加テスト手順：<2> 8.3.10.1。*** 顧客ユーザアクセスの唯一の認証要素としてパスワード／パスフレーズを使用する場合、システム構成設定を検査し、パスワード／パスフレーズがこの要件で指定される要素のいずれかに従って管理されていることを検証する。	パスワード／パスフレーズを唯一の認証要素として使用すると、漏洩した場合に単一障害点となる。したがって、これらの実装では、漏洩したパスワード／パスフレーズを介して悪意ある活動が発生する時間を最小限に抑えるための制御が必要である。 **グッドプラクティス** パスワード／パスフレーズを変更せずに長期間有効な場合、悪意のある人物にパスワード／パスフレーズを解読される時間が長くなります。定期的にパスワードを変更することで、悪意のある個人がパスワード／パスフレーズを解読する時間を短縮し、漏洩したパスワードを使用する時間を短縮することができます。 アカウントのセキュリティ状態を動的に分析することは、漏洩した可能性のある認証情報をより迅速に検出し、対応することを可能にするもう一つの選択肢である。このような分析では、デバイスの完全性、場所、アクセス時間、およびアクセスされたリソースを含む多くのデータポイントを使用して、要求されたリソースへのアクセスをアカウントが許可されるかどうかをリアルタイムで判断します。このようにして、アカウント情報の漏洩が疑われる場合、アクセスを拒否し、アカウントをブロックすることができる。 *(次ページに続く)*
カスタマイズアプローチの目的		
サービス提供者の顧客のパスワード／パスフレーズを無期限に使用できない。		
適用性の注記		
この要件は、消費者ユーザが自身のペイメントカード情報にアクセスするアカウントには適用されない。 *この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要があります。* *(次ページに続く)*		

要件とテスト手順		ガイダンス
この要件が 2025 年 3 月 31 日に発効するまでは、サービスプロバイダは要件 8.3.10 または 8.3.10.1 のいずれかを満たすことができます。		**その他の情報** リソースへのユーザアクセスを管理するための動的解析の使用については、*NIST SP 800-207 ゼロトラストアーキテクチャ* を参照してください。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.3.11 物理的または論理的セキュリティトークン、スマートカード、または証明書などの認証要素が使用される場合。 • 認証要素は個々のユーザに割り当てられ、複数のユーザ間で共有されることはない。 • 物理的および／または論理的な管理により、意図されたユーザのみがその要素を使用してアクセスできることを保証する。	**8.3.11.a** システム構成の設定を調査し、及び／又は該当する場合は物理的な制御を観察し、意図したユーザのみがその要因を使用してアクセスできることを保証するための制御が実施されていることを検証する。 **8.3.11.b** セキュリティ担当者にインタビューし、認証要素が個々のユーザに割り当てられ、複数のユーザ間で共有されていないことを確認する。 **8.3.11.c** システム構成設定および／または物理的管理（該当する場合）を調査し、意図されたユーザのみがその要素を使用してアクセスできることを保証するための管理が実施されていることを検証する。	トークン、スマートカード、証明書などの認証要素を複数のユーザが使用できる場合、認証メカニズムを使用している個人を特定できないことがあります。 **グッドプラクティス** アカウントのユーザを一意に認証するための物理的および／または論理的な管理（例えば、PIN、生体データ、パスワード）を行うことで、未承認のユーザが共有認証要素を使用してユーザアカウントにアクセスすることを防止することができます。
カスタマイズアプローチの目的		
認証因子は、それが割り当てられているユーザ以外には使用できない。		

要件とテスト手順		ガイダンス
8.4 カード会員データ環境（CDE）へのアクセスを保護するために、多要素認証（MFA）が実装されている。		
定義されたアプローチの要件 **8.4.1** 管理者アクセスを持つ担当者のカード会員データ環境（CDE）へのすべての非コンソールアクセスに MFA が実装されています。 **カスタマイズアプローチの目的** カード会員データ環境（CDE）への管理アクセスは、単一の認証要素を使用して取得することはできません。	**定義されたアプローチのテスト手順** **8.4.1.a** ネットワークおよび／またはシステム構成を調査し、管理者アクセス権を持つ担当者の CDE へのすべての非コンソールに MFA が必要であることを確認する。 **8.4.1.b** 管理者が CDE にログインしているところを観察し、MFA が必要であることを確認する。	**目的** 複数の認証要素を必要とすることで、攻撃者が複数の認証要素を侵害する必要があるため、正規のユーザを装ってシステムにアクセスできる確率を減らすことができます。これは、従来、パスワードやパスフレーズなど、ユーザが知っている認証要素が 1 つしか採用されていなかった環境において、特に当てはまります。 **定義** 1 つの要素を 2 回使用する（例えば、2 つの別々のパスワードを使用する）ことは、多要素認証とはみなされない。

要件とテスト手順		ガイダンス
適用性の注記 コンソール以外の管理者アクセスに対する MFA の要件は、昇格または増加した特権を持つすべての担当者が、コンソール以外の接続、つまり、直接的な物理接続ではなく、ネットワークインターフェース経由で発生する論理アクセスによりカード会員データ環境（CDE）にアクセスする場合に適用されます。 MFA は、カード会員データ環境（CDE）の一部ではない、対象システムコンポーネントへの非コンソール型管理者アクセスにおけるベストプラクティスと考えられています。		
定義されたアプローチの要件 **8.4.2** カード会員データ環境（CDE）へのすべてのアクセスに MFA が実装されている。	**定義されたアプローチのテスト手順** **8.4.2.a** ネットワークおよび／またはシステム構成を調べ、カード会員データ環境（CDE）へのすべてのアクセスに MFA が実装されていることを確認する。	**目的** 複数の認証要素を必要とすることで、攻撃者が複数の認証要素を侵害する必要があるため、正規のユーザを装ってシステムにアクセスできる確率を減らすことができます。これは、従来、パスワードやパスフレーズなど、ユーザが知っている認証要素が 1 つしか採用されていなかった環境において、特に当てはまります。 **定義** 1 つの要素を 2 回使用する（例えば、2 つの別々のパスワードを使用する）ことは、多要素認証とはみなされない。
	8.4.2.b カード会員データ環境（CDE）にログインする担当者を観察し、MFA が必要であることを検証するための証拠を調査する。	
カスタマイズアプローチの目的 カード会員データ環境（CDE）へのアクセスは、単一の認証因子の使用では取得できない。		

要件とテスト手順		ガイダンス
適用性の注記 この要件は、以下のものには適用されない。 • 自動化された機能を実行するアプリケーションまたはシステムアカウント。 • 1 回の取引を促進するために一度に 1 つのカード番号にのみアクセスできる POS 端末のユーザアカウント（POS 端末のレジ係が使用する ID など）。 要件 8.4.2 と要件 8.4.3 で指定された両方のタイプのアクセスに MFA が必要である。したがって、一方のタイプのアクセスに MFA を適用しても、他方のタイプのアクセスに MFA の別のインスタンスを適用する必要性に取って代わることはない。 ある個人が最初にリモートアクセスによって事業体のネットワークに接続し、その後ネットワーク内からカード会員データ環境（CDE）への接続を開始した場合、この要件に従って、その個人は 2 回 MFA を使用して認証します。1 回は事業体のネットワークにリモートアクセスで接続するとき、そして 1 回は事業体のネットワークからカード会員データ環境（CDE）に非コンソール管理アクセスで接続するときです。 *(次ページに続く)*		

要件とテスト手順		ガイダンス
MFA 要件は、クラウド、ホスティングシステム、オンプレミスアプリケーション、ネットワークセキュリティ機器、ワークステーション、サーバ、エンドポイントなど、あらゆるタイプのシステムコンポーネントに適用され、企業のネットワークやシステムへの直接アクセス、アプリケーションや機能へのウェブ ベースアクセスも含まれます。 カード会員データ環境（CDE）へのリモートアクセスのための MFA は、ネットワークまたはシステム／アプリケーションのレベルで実装することができます。例えば、ユーザがカード会員データ環境（CDE）のネットワークに接続する際に MFA を使用する場合、ユーザがカード会員データ環境（CDE）内の各システムまたはアプリケーションにログインする際に MFA を使用する必要はありません。 この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要があります。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.4.3 カード会員データ環境（CDE）にアクセスまたは影響を与える可能性のある、事業体のネットワーク外から発信されるすべてのリモートネットワークアクセスに対して、以下のように多要素認証が実施される。 • ユーザ権限および管理者権限を有するすべての担当者による、事業体のネットワーク外から発信されるすべてのリ モートアクセス。 • サードパーティーおよびベンダによるすべてのリモートアクセス。	**8.4.3.a** リモートアクセスサーバおよびシステムのネットワークおよび／またはシステム構成を調べ、この要件で指定されたすべての要素に従って多要素認証が必要であることを確認する。 **8.4.3.b** ネットワークにリモート接続する担当者（例えば、ユーザや管理者）を観察し、多要素認証が必要であることを確認する。	認証要素を複数種類要求することで、攻撃者が複数の認証要素を侵害する必要が生じ、正規のユーザを装ってシステムにアクセスできる確率を減らすことができます。これは、従来、パスワードやパスフレーズなど、ユーザが知っている認証要素が 1 つしか採用されていなかった環境において、特に当てはまります。 **定義** 多要素認証(MFA）は、アクセスを許可する前に、個人が要件 8.3.1 で指定された 3 つの認証要素のうち最低 2 つを提示することを要求します。1 つの要素を 2 回使用する（たとえば、2 つの別々のパスワードを使用する）ことは、多要素認証とはみなされません。
カスタマイズアプローチの目的 単一認証要素では、事業体のネットワークへのリモートアクセスは取得できない。		
適用性の注記 事業体のネットワーク外から発生するリモートアクセスに対する多要素認証の要件は、リモートアクセスがカード会員データ環境（CDE）へのアクセスにつながる、またはつながる可能性がある、ネットワークにリモートアクセスできるすべてのユーザアカウントに適用される。		

(次ページに続く)

要件とテスト手順		ガイダンス
リモートアクセスがカード会員データ環境（CDE）から適切にセグメント化され、リモートユーザがカード会員データ環境（CDE）にアクセスまたは影響を与えることができないような事業体ネットワークの一部である場合、ネットワークのその部分へのリモートアクセスに対する MFA は必要ではない。しかし、カード会員データ環境（CDE）にアクセスするネットワークへのリモートアクセスには多要素認証が必要であり、事業体のネットワークへのすべてのリモートアクセスに多要素認証が推奨される。 多要素認証の要件は、クラウド、ホスティングシステム、オンプレミスアプリケーション、ネットワークセキュリティ機器、ワークステーション、サーバ、エンドポイントなど、あらゆるタイプのシステムコンポーネントに適用され、事業体のネットワークやシステムへの直接アクセス、アプリケーションや機能への Web ベースアクセスも含まれる。		

要件とテスト手順		ガイダンス
8.5 多要素認証。(MFA)システムが悪用されないように構成されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.5.1 多要素認証システムは、以下のように実装される。 • 多要素認証システムはリプレイ攻撃の影響を受けない • 多要素認証システムは、期間を限定して、特別に文書化し、例外的に管理者によって許可されない限り、管理者ユーザを含むいかなるユーザであってもバイパスすることはできない • 少なくとも異なる 2 種類の認証要素が使用されている • アクセスが許可される前に、すべての認証要素に成功することが要求される	**8.5.1.a** ベンダのシステム文書を調べ、多要素認証システムがリプレイ攻撃の影響を受けないことを確認する。	多要素認証システムの設定が不十分な場合、攻撃者にバイパスされる可能性があります。したがって、この要件は、カード会員データ環境（CDE）内のシステムコンポーネントにアクセスするユーザに多要素認証を提供する多要素認証システムの構成に対応します。
	8.5.1.b 多要素認証を実装するシステム構成を調べ、この要件で指定されたすべての要素に従って構成されていることを確認する。	**定義** 1 つの要素を 2 回使用する（例えば、2 つの別々のパスワードを使用する）ことは、多要素認証とはみなされません。
	8.5.1.c 担当者にインタビューし、プロセスを観察して、多要素認証をバイパスする要求が、期間を限定し、特別に文書化され、例外として管理者によって承認されることを確認する。	**その他の情報** MFA の仕組みや機能については、以下をご参照ください。 *PCI SSC の情報補足：多要素認証* このトピックに関する PCI SSC のよくある質問（FAQ）。
	8.5.1.d カード会員データ環境（CDE） のシステムコンポーネントにログインする担当者を観察し、すべての認証要素に成功した後にのみアクセスが許可されることを確認する。	
カスタマイズアプローチの目的	**8.5.1.e** 組織のネットワーク外からリモートで接続する担当者を観察し、すべての認証要素に成功した後にのみアクセスが許可されることを確認する。	
多要素認証システムは攻撃に強く、管理上の無効化を厳しく管理する。		

要件とテスト手順		ガイダンス
適用性の注記		
この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要があります。		

要件とテスト手順		ガイダンス
8.6 アプリケーションおよびシステムアカウントの使用、および関連する認証要素を厳密に管理する。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
8.6.1 システムやアプリケーションで使用されるアカウントが対話型ログインに使用できる場合、以下のように管理される。 • 例外的に必要な場合を除き、インタラクティブな使用を禁止する • インタラクティブな使用は、例外的な状況で必要とされる時間内に制限される • インタラクティブな使用を正当化するビジネス上の理由が文書化されている • インタラクティブな使用は、経営陣が明示的に承認している • アカウントへのアクセスが許可される前に、個々のユーザの身元が確認される • 実行されたすべてのアクションは、個々のユーザに帰属する	**8.6.1** アプリケーションとシステムアカウントがこの要件で指定されたすべての要素に従って管理されていることを確認するために、対話的に使用できるアプリケーションとシステムアカウントを調べ、管理担当者にインタビューする。	システムアカウントやアプリケーションアカウントは、個々のユーザアカウントと同様に、意図した目的のみに使用され、悪用されないよう、説明責任と厳密な管理が必要です。 攻撃者はしばしば、カード会員データにアクセスするためにシステムまたはアプリケーションのアカウントを侵害します。 **グッドプラクティス** 可能であれば、システムおよびアプリケーションのアカウントは、権限のない個人がログインして、そのアカウントに関連するシステム特権を使用することを防ぐために、対話型ログインを禁止するように設定し、アカウントが使用できるマシンおよびデバイスを制限します。 **定義** システムまたはアプリケーションアカウントとは、コンピュータシステムまたはアプリケーション上でプロセスを実行したり、タスクを実行するアカウントであり、通常、個人がログオンするアカウントではありません。これらのアカウントは通常、特殊なタスクや機能を実行するために必要な、昇格された権限を有しています。 *(次ページに続く)*
カスタマイズアプローチの目的		
インタラクティブに使用される場合、システムまたはアプリケーションアカウントとして指定されたアカウントでのすべてのアクションは許可され、個人に帰属しなければならない。		

要件とテスト手順		ガイダンス
適用性の注記 この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要があります。		対話型ログインとは、通常のユーザアカウントと同じ方法で、システムまたはアプリケーションアカウントにログインする機能です。システムおよびアプリケーションアカウントをこのように使用することは、ユーザによって行われた行為の説明責任およびトレーサビリティがないことを意味する。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
8.6.2 対話型ログインに使用できるアプリケーションおよびシステムアカウント用のパスワード／パスフレーズは、スクリプト、構成ファイル／プロパティファイル、カスタムソースコードにハードコードされていてはならない。	**8.6.2.a** 担当者にインタビューし、システム開発手順を調査して、対話型ログインに使用できるアプリケーションおよびシステムアカウントについて、スクリプト、構成ファイル／プロパティファイル、またはカスタムソースコードにパスワード／パスフレーズがハードコーディングされていないことを指定したプロセスが定義されていることを確認する。	**目的** アプリケーションやシステムのアカウントで使用されるパスワード／パスフレーズを適切に保護しない場合、特にそれらのアカウントが対話型ログインに使用できる場合は、それらの特権アカウントの不正使用のリスクと成功率が増加します。 **グッドプラクティス** 漏洩の疑いや確認により、これらの値を変更することは特に困難です。 ツールは、アプリケーションとシステムアカウントの認証要素の管理とセキュリティの両方を容易にすることができます。例えば、パスワード保管庫や他のシステムで管理されたコントロールを検討します。
	8.6.2.b 対話型ログインに使用できるアプリケーションおよびシステムアカウントについて、スクリプト、設定／プロパティファイル、特注およびカスタムソースコードを調べ、これらのアカウントのパスワード／パスフレーズが存在しないことを確認する。	
カスタマイズアプローチの目的 アプリケーションおよびシステムアカウントで使用されているパスワード／パスフレーズが、権限のない者に使用されないようにする。		
適用性の注記 保存されているパスワード／パスフレーズは、PCI DSS 要件 8.3.2 に従って暗号化する必要があります。 *この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要があります。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** システムおよびアプリケーションアカウントは、データベースへのプログラムアクセスなど、通常ユーザアカウントに付与されないシステムへのアクセスを伴う、高度なセキュリティコンテキストで実行されることが多いため、ユーザアカウントよりも固有のセキュリティリスクをもたらす。そのため、アプリケーションやシステムアカウントに使用されるパスワードやパスフレーズを保護するために、特別な配慮が必要である。 **グッドプラクティス** 事業体は、アプリケーションおよびシステムのパスワード／パスフレーズを誤用から保護する方法を決定する際に、以下のリスク要因を考慮する必要があります。 • パスワード／パスフレーズがどの程度安全に保管されているか（例えば、パスワード保管庫に保管されているかどうか） • スタッフの離職率 • 認証要素にアクセスできる人の数 • アカウントが対話型ログインに使用できるかどうか • アカウントのセキュリティ状態が動的に分析され、それに応じてリソースへのリアルタイムアクセスが自動的に決定されるかどうか（要件 8.3.9 を参照） *(次ページに続く)*
8.6.3 アプリケーションおよびシステムアカウント用のパスワード／パスフレーズは、次のように悪用から保護されます。 • パスワード／パスフレーズは定期的に（要件 12.3.1 に規定されるすべての要素に従って実行される事業体のターゲットリスク分析で定義される頻度で）、および侵害の疑いまたは確認があった場合に変更される • パスワード／パスフレーズは、事業体がパスワード／パスフレーズを変更する頻度 に応じて、十分な複雑さで構築されている	**8.6.3.a** ポリシーと手順を調査し、この要件で指定されたすべての要素に従って、アプリケーションまたはシステムアカウントのパスワード／パスフレーズを悪用から保護するための手順が定義されていることを確認する。	
	8.6.3.b アプリケーションおよびシステムアカウントへの対話型ログインに使用されるパスワード／パスフレーズの変更頻度および複雑性に関する事業体のターゲットリスク分析を調べ、リスク分析が要件 12.3.1 に規定されるすべての要素およびアドレスに従って実施されたことを確認する。 • アプリケーションおよびシステムのパスワード／パスフレーズを定期的に変更するために定義された頻度。 • パスワード／パスフレーズに定義された複雑さと、変更頻度に対する複雑さの妥当性。	
カスタマイズアプローチの目的	**8.6.3.c** 担当者にインタビューを行い、システム構成設定を調査して、対話型ログインに使用できるすべてのアプリケーションおよびシステムアカウントのパスワード／パスフレーズが、この要件で指定されているすべての要素に従って悪用から保護されていることを確認する。	
アプリケーションとシステムアカウントで使用されるパスワード／パスフレーズは、無期限に使用することはできず、ブルートフォース攻撃と推測攻撃に耐えられるように構造化されている。		

要件とテスト手順		ガイダンス
適用性の注記 *この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要があります。*		これらの要素はすべて、アプリケーションおよびシステムアカウントのリスクレベルに影響を与え、システムおよびアプリケーションアカウントによってアクセスされるシステムのセキュリティに影響を与える可能性があります。 事業体は、アプリケーションおよびシステムのパスワード／パスフレーズの変更頻度を、それらのパスワード／パスフレーズの複雑さと関連付けるべきです。すなわち、パスワード／パスフレーズの変更頻度が低い場合は複雑さをより厳しくし、変更頻度が高い場合は厳しさを軽減することができます。例えば、パスワード／パスフレーズの複雑さを、大文字と小文字、数字、特殊文字を含む 36 文字の英数字に設定した場合、変更頻度を長くすることがより正当化されます。 ベストプラクティスは、パスワードの変更を少なくとも年に 1 回、パスワード／パスフレーズの長さを 15 文字以上、パスワード／パスフレーズの複雑さを英数字、大文字、小文字、特殊文字で設定することを検討することです。 **その他の情報** 異なる形式のパスワード／パスフレーズに対するパスワード強度のばらつきと同等性については、業界標準（たとえば、最新版の *NIST SP 800-63 デジタルアイデンティティガイドライン*）を参照してください。

要件 9:　　カード会員データへの物理アクセスを制限する

セクション
9.1 カード会員データへの物理的なアクセスを制限するためのプロセスおよびメカニズムが定義され、理解されている。
9.2 物理的なアクセス制御により、カード会員データを含む施設およびシステムへの入館を管理する。
9.3 担当者および訪問者の物理的なアクセスは許可され、管理されている。
9.4 カード会員データを含むメディアは、安全に保管、アクセス、配布、および破棄される。
9.5 POI 端末は、改ざんや不正な置き換えから保護されている。

概要

カード会員データまたはカード会員データを保存、処理、伝送するシステムへの物理的なアクセスは、 カード会員データを含むシステムまたはハードコピーへのアクセスまたは削除の機会を提供するため、 物理的なアクセスは適切に制限される必要があります。

要件 9 には、3 つの異なる領域が記載されています。

1. 機密性の高い領域に特に言及している要件は、その領域のみに適用されることを意図しています。
2. カード会員データ環境（CDE）に特に言及している要件は、カード会員データ環境（CDE） 内に存在するすべての機密エリアを含むカード会員データ環境（CDE） 全体に適用されることを意図しています。
3. 施設に特に言及している要件は、カード会員データ環境（CDE）および機密エリアが存在する事業所（建物など）の物理的な境界で、より広範に管理される可能性があるタイプの管理を参照しています。これらの管理は、例えば、訪問者を識別し、バッジを付け、記録する警備員室のように、カード会員データ環境（CDE）または機密領域の外部に存在することが多いです。「施設」という用語は、これらの管理が施設内の異なる場所、例えば、建物の入口、データセンターまたは オフィススペースの内部入口に存在し得ることを認識するために使用されます。

「メディア（media）」、「担当者（personnel）」、「機密エリア（sensitive areas）」、およびその他の PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
9.1 カード会員データへの物理的なアクセスを制限するためのプロセスおよびメカニズムが定義され、理解されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.1.1 要件 9 で特定されるすべてのセキュリティポリシーと運用手順がある。 • 文書化されている • 最新の状態に保たれている • 使用されている • すべての関係者に知られている	**9.1.1** 要件 9 で指定されているセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認するために、文書を調査し、担当者にインタビューする。	要件 9.1.1 は、要件 9 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 9 に掲げられた特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及していることを確認することも同様に重要です。 **グッドプラクティス** プロセス、技術、ビジネス目的の変化に対応するため、ポリシーと手順を必要に応じて更新することが重要です。そのため、定期的な更新だけでなく、変更が発生したらできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、事業体のセキュリティの目的および原則を定義します。運用手順は、アクティビティの方法を説明し、一貫した方法で、かつ、ポリシーの目的に沿って望ましい結果を達成するために従う統制、方法、プロセスを定義しています。 ポリシーおよび手順は、更新を含め、影響を受けるすべての担当者に積極的に伝達され、アクティビティの実行方法を記述した運用手順によってサポートされています。
カスタマイズアプローチの目的		
要件 9 内のアクティビティを満たすために期待されること、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべてのサポートアクティビティが繰り返し適用可能であり、一貫して用いられ、経営者の意図に適合している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.1.2 要件 9 のアクティビティを行うための役割と責任が文書化され、割り当てられ、理解されている。	**9.1.2.a** 文書を調査し、要件 9 のアクティビティを行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要なアクティビティが行われない可能性があります。 **グッドプラクティス** 役割と責任は、ポリシーと手順の中で文書化されるか、または別の文書で管理されるかもしれません。 役割と責任を伝える一環として、事業体は担当者が与えられた役割と責任を受け入れ理解したことの確認を検討することができます。 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担マトリックス（RACI マトリックスとも呼ばれる） があります。
カスタマイズアプローチの目的	**9.1.2.b** 要件 9 のアクティビティの実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
要件 9 のすべてのアクティビティを実行するための日常的な責任が割り当てられている。担当者は、これらの要件の達成と継続的な運用に責任を負う。		

要件とテスト手順		ガイダンス
9.2 物理的なアクセス制御により、カード会員データを含む施設およびシステムへの入館を管理する。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.2.1 カード会員データ環境（CDE）内のシステムへの物理的アクセスを制限するために、適切な施設入館管理が実施されている。	**9.2.1** カード会員データ環境（CDE）内のシステムへのアクセスを制限するための物理的なセキュリティ管理が行われていることを確認するために、入室管理を観察し、担当者にインタビューする。	物理的なアクセス制御を行わない場合、権限のない者がカード会員データ環境（CDE）や機密情報にアクセスしたり、システム設定の変更、ネットワークへの脆弱性の導入、機器の破壊や窃盗を行う可能性があります。したがって、この要件の目的は、カード会員データ環境（CDE）への物理的なアクセスが、バッジ読み取り機などの物理的なセキュリティコントロール、または錠前と鍵などの他のメカニズムによって制御されることです。
カスタマイズアプローチの目的		**グッドプラクティス**
カード会員データ環境（CDE）内のシステムコンポーネントは、権限のない者が物理的にアクセスすることができない。		どのメカニズムがこの要件を満たす場合でも、組織が許可された担当者のみにアクセスが許可されていることを確認するのに十分なものでなければなりません。
		例
		施設入室管理には、各コンピュータ室、データセンター、およびカード会員データ環境（CDE）内のシステムがあるその他の物理的エリアにおける物理的なセキュリティ管理が含まれます。また、バッジ読み取り機や、鍵を保有している全ての個人の最新リストとともに錠前と鍵で管理するなど、物理的なアクセス制御で管理する他のデバイスを含めることもできます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
9.2.1.1 カード会員データ環境（CDE）内の機密エリアへの個々の物理的アクセスは、以下のようにビデオカメラまたは物理的アクセス制御機構（またはその両方）で監視される。 • カード会員データ環境（CDE）内の機密エリアへの／からの出入口は監視される • 監視装置または機構は、改ざんまたは無効化されないように保護されている • 収集されたデータは、レビューされ、他のエントリと関連付けられる • 収集されたデータは、法律による制約がない限り、少なくとも 3 カ月間保管される	**9.2.1.1.a** CDE 内の機密エリアへの個人の物理的アクセスが発生する場所を観察し、出入口を監視するためにビデオカメラまたは物理的アクセス制御メカニズム（またはその両方）が設置されていることを確認する。	**目的** 機密エリアに出入りした個人の詳細を記録することで、物理的に機密エリアにアクセスした個人と、いつ入退出したかを特定し、物理的な侵害の調査に役立てることができます。 **グッドプラクティス** どのようなメカニズムであれ、この要件を満たすには、機密エリアへのすべての出入口を効果的に監視する必要があります。 機密エリアへの物理的アクセスを試みる犯罪者は、しばしば監視制御を無効化またはバイパスしようとします。これらの制御を改ざんから守るために、ビデオカメラを手の届かないところに設置したり、改ざんを検知できるように監視したりすることが考えられます。同様に、物理的なアクセス制御機構は、悪意のある個人による損傷や無効化を防ぐために、監視されたり、物理的な保護装置を設置したりすることができます。
	9.2.1.1.b CDE 内の機密エリアへの個人の物理的アクセスが発生する場所を観察し、ビデオカメラまたは物理的アクセス制御機構（またはその両方）が、改ざんまたは無効化から保護されていることを確認すること。	
カスタマイズアプローチの目的	**9.2.1.1.c** 物理的なアクセス制御機構を観察し、および/または、ビデオカメラを調べ、担当者にインタビューして、それを検証する。 • ビデオカメラおよび／または物理的アクセス制御機構から収集されたデータは、レビューされ、他のエントリと関連付けられる。 • 収集されたデータは、少なくとも 3 カ月間保管される。	
機密エリアへの個人の物理的な入退出について、信頼でき検証可能な記録が維持されている。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.2.2 施設内の誰でもアクセス可能なネットワークジャックの使用を制限するために、物理的および／または論理的な管理が実施されている。	**9.2.2** 責任者にインタビューし、誰でもアクセス可能なネットワークジャックの場所を観察し、施設内の誰でもアクセス可能なネットワークジャックへのアクセスを制限するための物理的および／または論理的管理が実施されていることを確認する。	ネットワークジャック（またはネットワークポート）へのアクセスを制限することで、悪意のある個人が簡単に利用できるネットワークジャックにプラグを差し込み、カード会員データ環境（CDE）またはカード会員データ環境（CDE）に接続されたシステムにアクセスすることを防止します。
カスタマイズアプローチの目的		**グッドプラクティス**
未許可のデバイスが施設内の公共エリアから事業体のネットワークに接続できないこと。		論理的管理か物理的管理か、あるいはその両方の組み合わせかを問わず、明示的に許可されていない個人またはデバイスがネットワークに接続できないようにする必要があります。
		例
		この要件を満たす方法としては、公共エリアや訪問者がアクセスできるエリアにあるネットワークジャックを無効にし、ネットワークアクセスが明示的に許可された場合にのみ有効にすることができます。または、ネットワークジャックが有効なエリアでは、訪問者が常にエスコートされていることを確認するプロセスを導入することも可能です。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **9.2.3** 施設内の無線アクセスポイント、ゲートウェイ、ネットワーク／通信ハードウェア、通信回線への物理的なアクセスは制限される。 **カスタマイズアプローチの目的** 物理的なネットワーク機器に、権限のない者がアクセスすることはできない。	**定義されたアプローチのテスト手順** **9.2.3** 担当者にインタビューし、ハードウェアと回線の場所を観察して、施設内の無線アクセスポイント、ゲートウェイ、ネットワーキング／通信ハードウェア、および通信回線への物理的なアクセスが制限されていることを確認する。	**目的** 無線設備や機器、コンピュータネットワークや通信機器、回線へのアクセスに適切な物理的セキュリティがなければ、悪意のあるユーザが事業体のネットワークリソースにアクセスする可能性があります。また、悪意のあるユーザが自身の機器をネットワークに接続し、カード会員データ環境（CDE）やカード会員データ環境（CDE）に接続されたシステムに不正にアクセスする可能性があります。 さらに、ネットワークおよび通信用ハードウェアを保護することにより、悪意のあるユーザがネットワークトラフィックを傍受したり、自身の機器を有線ネットワークリソースに物理的に接続したりすることを防止します。
定義されたアプローチの要件 **9.2.4** 機密エリアにあるコンソールへのアクセスは、使用されていないときはロックにより制限される。 **カスタマイズアプローチの目的** 機密エリア内の物理コンソールを権限のない者が使用できないようにする。	**定義されたアプローチのテスト手順** **9.2.4** システム管理者が機密エリアのコンソールにログインしようとする試行を観察し、不正使用を防止するために「ロック」されていることを確認する。	**目的** コンソールのログイン画面をロックすることで、権限のない者が機密情報へのアクセス、システム設定の変更、ネットワークへの脆弱性の導入、記録の破壊を防ぐことができます。

要件とテスト手順		ガイダンス
9.3 担当者および訪問者の物理的なアクセスは許可され、管理されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** アクセス権の付与、管理、および不要になった場合の削除の手順を確立することにより、権限のない個人がカード会員データを含む領域にアクセスすることを確実に防止することができます。さらに、実際のバッジシステムおよびバッジ材料へのアクセスを制限して、権限のない担当者が独自のバッジを作成したり、独自のアクセスルールを設定したりすることを防止することが重要です。 **グッドプラクティス** 物理的に存在する担当者と、その人物が訪問者なのか従業員なのかを視覚的に識別することが重要です。 **例** 担当者を特定する一つの方法として、バッジを付与することがあります。
9.3.1 カード会員データ環境（CDE）への担当者の物理的アクセスを許可および管理するために、以下のような手順が実施されている。 • 担当者の識別 • 個人の物理アクセス要件の変更を管理する • 担当者の ID の失効または終了 • 識別プロセスまたはシステムへのアクセスを許可された担当者に限定する	**9.3.1.a** 文書化された手順を調査し、CDE への人員の物理的アクセスを承認および管理する手順が、この要件で指定されているすべての要素に従って定義されていることを検証する。	
	9.3.1.b ID バッジなどの識別方法とプロセスを観察し、CDE 内の要員が明確に識別されていることを確認する。	
カスタマイズアプローチの目的	**9.3.1.c** バッジシステムなどの識別プロセスへのアクセスが許可された人員に限定されていることを確認するために、プロセスを観察する。	
物理的なカード会員データ環境（CDE）へのアクセスに関する要件が定義され、担当者の識別と許可のために実施されている。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.3.1.1 カード会員データ環境（CDE）内の機密エリアへの担当者の物理的アクセスは、以下のように管理されている。 • アクセスは、個人の職務権限に基づき許可される • アクセスは、職務の終了後に直ちに取り消される • 鍵、アクセスカードなどのすべての物理的なアクセス機構は、職務の終了後に返却または無効化される	**9.3.1.1.a** カード会員データ環境（CDE）内の機密エリアにいる担当者を観察し、責任者にインタビューし、物理アクセス制御リストを調査して、以下を確認する。 • 機密エリアへのアクセスが許可されていること。 • アクセスは、個人の職務上必要であること。	機密エリアへの物理的なアクセスを制御することで、正当なビジネスニーズを持つ許可された担当者のみがアクセスを許可されることを保証することができます。 **グッドプラクティス** 可能であれば、組織は、従業員が退職する前に、すべての物理的アクセス機構を返却するか、または退職後できるだけ早く無効にするためのポリシーと手順を持つべきである。これにより、担当者はその雇用が終了した後、機密エリアへの物理的なアクセスを得ることができなくなる。
カスタマイズアプローチの目的	**9.3.1.1.b** プロセスを観察し、担当者にインタビューし、すべての担当者のアクセスが離職時に直ちに取り消されることを確認する。	
機密エリアは、権限のない者がアクセスすることはできない。	**9.3.1.1.c** 離職した担当者について、物理的なアクセス制御リストを調査し、担当者にインタビューを行い、すべての物理的なアクセス機構（鍵、アクセスカードなど）が返却または無効にされたことを確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
9.3.2 カード会員データ環境（CDE）への訪問者のアクセスを承認し管理するために、以下のような手順が実施されている。 • 訪問者は、入館前に承認される • 訪問者は、常に付き添われている • 訪問者は、明確に識別され、有効期限付きバッジその他の ID が渡される • 訪問者のバッジまたはその他の識別情報は、訪問者と職員とを目に見える形で区別する	**9.3.2.a** 文書化された手順を調べ、担当者にインタビューし、この要件で指定されたすべての要素に従って、カード会員データ環境（CDE）への訪問者のアクセスを承認および管理するための手順が定義されていることを確認する。	**目的** 無許可の悪意ある人物による施設へのアクセス、およびカード会員情報へのアクセスを減らすために、訪問者の管理は重要です。 訪問者の管理では、訪問者を訪問者として識別できるようにして、担当者が訪問者の行動を監視できるようにし、訪問者のアクセスを正規の訪問期間だけに制限します。
	9.3.2.b カード会員データ環境（CDE）に来訪者がいる場合のプロセスを観察し、担当者にインタビューして、来訪者が以下の通りであることを確認する。 • カード会員データ環境（CDE）に入る前に認可されていること。 • カード会員データ環境（CDE）内では常に付き添われていること。	
	9.3.2.c 来訪者バッジまたはその他の身分証明書の使用を観察し、そのバッジまたはその他の身分証明書があったとしても付き添いなしではカード会員データ環境（CDE）に入ることは許可されていないことを確認する。	

要件とテスト手順		ガイダンス
	9.3.2.d カード会員データ環境（CDE）内の訪問者を観察し、以下を確認する。 • すべての訪問者に訪問者バッジまたは他の ID が使用されていること。 • 訪問者バッジまたは身分証明書は、訪問者と職員とを容易に区別することができる。	
カスタマイズアプローチの目的 カード会員データ環境（CDE）への訪問者のアクセスに関する要件が定義され、実施される。カード会員データ環境（CDE）にいる間、訪問者は許可された物理アクセス以上のアクセスをすることはできない。	**9.3.2.e** 訪問者バッジまたはその他の身分証明書を検査し、バッジシステム内の証拠を観察して、訪問者バッジまたはその他の身分証明書の有効期限を確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **9.3.3** 訪問者バッジまたは身分証明書は、訪問者が施設を出る前、または有効期限が切れた時点で引き渡し、または無効化される。 **カスタマイズアプローチの目的** 来訪者の身分証明書やバッジは、有効期限を過ぎると再利用できない。	**定義されたアプローチのテスト手順** **9.3.3** 施設から出て行く訪問者を観察し、職員にインタビューして、訪問者バッジまたはその他の身分証明書が、訪問者が施設を出る前または有効期限が切れた時点で放棄または無効化されていることを確認する。	**目的** 訪問者バッジが、有効期限または訪問終了時に返却または無効化されることを確実にすることで、悪意ある人物が、訪問終了後に、以前に許可されたパスを使用して建物に物理的にアクセスすることを防止します。
定義されたアプローチの要件 **9.3.4** 訪問者記録は、施設内および機密エリア内での訪問者のアクティビティに関する物理的な記録を維持するために使用される。 • 訪問者の名前と代表する組織 • 訪問日時。物理的なアクセスを許可した担当者の名前 • 法律で制限されていない限り、少なくとも 3 カ月間ログを保持すること **カスタマイズアプローチの目的** 個人を特定できるような訪問者のアクセス記録が維持されている。	**定義されたアプローチのテスト手順** **9.3.4.a** 施設および機密エリアへの物理的アクセスを記録するために訪問者ログが使用されていることを確認するために、訪問者ログを調べ、責任者にインタビューする。 **9.3.4.b** 訪問者ログを調べ、そのログに以下の内容が含まれていることを確認する。 • 訪問者の名前と代表する組織。 • 物理的なアクセスを許可する担当者。 • 訪問の日付と時間。 **9.3.4.c** 訪問者ログの保管場所を調査し、責任者にインタビューし、ログが、法律で制限されていない限り、少なくとも 3 カ月間保管されていることを確認する。	**目的** 訪問者に関する最低限の情報を記録した訪問者記録は、維持するのが簡単で安価である。これは、建物または部屋への過去の物理的なアクセス、およびカード会員データへの潜在的なアクセスを識別するのに役立ちます。 **グッドプラクティス** 訪問日時を記録する場合、入室時間と退室時間の両方を記録することは、有用な追跡情報を提供し、1 日の終わりに訪問者が退室したことを保証するため、ベストプラクティスと考えられています。また、訪問者の ID（運転免許証など）が訪問者ログに記入された名前と一致していることを確認するのもよい方法です。

要件とテスト手順		ガイダンス
9.4 カード会員データを含むメディアを安全に保管、アクセス、配布、破棄する。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.4.1 カード会員データのあるすべてのメディアは、物理的に安全である。	**9.4.1.** 文書を調査し、カード会員データを保護するために定義された手順に、すべてのメディアを物理的に保 護するためのコントロールが含まれていることを検証する。	物理的にメディアを保護するためのコントロールは、権限のない人があらゆるメディア上のカード会員データにアクセスすることを防止することを目的としています。カード会員データは、リムーバブルメディアまたはポータブルメディアに保存されたり印刷されたり誰かの机上に放置されたりしている時に保護されていない場合、不正な閲覧やコピー、スキャンを受ける可能性があります。 安全でない施設に保管されている場合、カード会員データを含むバックアップは簡単に紛失、盗難、または悪意あるコピーにあう可能性があります。
カスタマイズアプローチの目的		
カード会員情報の入ったメディアは、権限のない者がアクセスすることはできません。		
9.4.1.1 カード会員データを含むオフラインメディアのバックアップは、安全な場所に保管される。	**9.4.1.1.a** 文書を調査し、カード会員データを含むオフラインメディアのバックアップを安全な場所に物理的に保護するための手順が定義されていることを確認する。	
	9.4.1.1.b ログまたはその他の文書を調査し、保管場所の責任者にインタビューして、オフラインメディアバックアップが安全な場所に保管されていることを確認する。	**グッドプラクティス** バックアップメディアを安全に保管するためには、代替施設やバックアップサイト、商業用保管施設など、オフサイトの施設にメディアを保管するのがよい方法です。
カスタマイズアプローチの目的		
オフラインバックアップは、権限のない者がアクセスすることはできない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.4.1.2 カード会員データを含むオフラインメディアのバックアップ場所のセキュリティは、少なくとも 12 カ月に 1 回見直される。	**9.4.1.2.a** カード会員データを含むオフラインメディアのバックアップ場所のセキュリティを少なくとも 12 カ月に 1 回レビューするための手順が定義されていることを確認するために、文書を調査する。	保管施設の定期的なレビューを実施することにより、組織は特定されたセキュリティ問題に迅速に対処し、潜在的なリスクを最小化することができます。事業体は、メディアが保管されている場所のセキュリティについて認識しておくことが重要です。
	9.4.1.2.b 文書化された手順、ログ、またはその他の文書を調査し、保管場所の責任者にインタビューして、保管場所のセキュリティが少なくとも 12 カ月に 1 回レビューされていることを確認する。	
カスタマイズアプローチの目的		
オフラインバックアップを保護するセキュリティ管理は、定期的に検査によって確認される。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.4.2 カード会員データを含むすべてのメディアは、データの機密性に応じて分類される。	**9.4.2.a** 文書を調査し、カード会員データを含むメディアをデータの機密性に従って分類するための手順が定義されていることを確認する。	機密扱いでないメディアは、適切に保護されていない可能性があり、紛失や盗難に遭う可能性があります。 **グッドプラクティス** メディアは、その分類状態が明らかになるように識別することが重要である。ただし、これはメディアに「機密」のラベルを貼る必要があることを意味するものではありません。
	9.4.2.b メディアのログまたはその他の文書を調査し、すべてのメディアがデータの機密性に応じて分類されていることを確認する。	
カスタマイズアプローチの目的		
メディアが適切に分類され、保護されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.4.3 施設外に送付されるカード会員データを含むメディアは、以下のように保護される。 *(次ページに続く)*	**9.4.3.a** 文書を調査し、この要件で指定されたすべての要素に従って、施設外に送られるメディアの安全確保のための手順が定義されていることを確認する。	通常の郵便のような追跡不可能な方法で送られた場合、メディアの紛失や盗難の可能性があります。カード会員データを含むメディアの配送に安全な配送業者を使用することで、組織は追跡シス

要件とテスト手順		ガイダンス
• 施設外に送られたメディアは記録される • メディアは、安全な宅配便または正確に追跡できるその他の配送方法で送付される • オフサイトの追跡ログには、メディアの場所に関する詳細が含まれる	**9.4.3.b** 施設外に送られる全ての媒体が記録され、追跡可能な保護された宅配便またはその他の配送方法で送られることを検証するため、担当者にインタビューを行い、 記録を調べるものとする。	テムを使用して配送品の在庫と場所を管理することができます。
カスタマイズアプローチの目的 施設外に輸送されるメディアは保護され、追跡されている。	**9.4.3.c** すべてのメディアのオフサイト追跡ログを調査し、追跡の詳細が文書化されていることを確認する。	
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.4.4 管理者は、施設外に移動されるカード会員データが含まれるすべてのメディアを承認する（メディアが個人に配布される場合を含む）。	**9.4.4.a** 文書を調査し、施設外に移動する媒体が管理者によって承認されることを確実にするための手順が定義されていることを確認する。	メディアを安全な場所から移動させる前に、すべてのメディアの移動が承認されることを確実にするための確固たるプロセスがなければ、メディアは追跡されず、適切に保護されず、その場所が不明となり、メディアの紛失や盗難につながるであろう。
カスタマイズアプローチの目的 説明責任者の承認なしに、メディアを施設外に持ち出すことはできない。	**9.4.4.b** 施設外に移動した全てのメディア（個人への配布メディアを含む）に対して適切な管理者の承認が得られていることを確認するため、施設外にあるメディアの追跡ログを調べ、担当者にインタビューする。	
適用性の注記 メディアの移動を承認する個人は、この承認を与えるための適切なレベルの管理権限を有するべきである。しかし、そのような個人が肩書きの一部として「マネージャー」を持つことは特に要求されない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 慎重な棚卸し方法と保管管理がなければ、盗まれたり紛失した電子メディアは、無期限に気づかれない可能性があります。
9.4.5 カード会員データのあるすべての電子メディアのインベントリログが維持されている。	**9.4.5.a** 電子メディアインベントリログを維持するための手順が定義されていることを確認するために、文書を調査する。	
	9.4.5.b 電子メディアインベントリログを調査し、担当者にインタビューして、ログが維持されていることを確認する。	
カスタマイズアプローチの目的 保管されている電子媒体の正確なインベントリが維持されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 慎重な棚卸し方法と保管管理がなければ、盗まれたり紛失した電子メディアは、無期限に気づかれない可能性があります。
9.4.5.1 カード会員データのある電子メディアのインベントリは、少なくとも 12 カ月に 1 回実施される。	**9.4.5.1.a** 文書を調査し、カード会員データを含む電子メディアのインベントリを少なくとも 12 カ月に 1 度実施する手順が定義 されていることを確認する。	
	9.4.5.1.b 電子メディアのインベントリログを調査し、担当者にインタビューして、電子メディアのインベントリが少なくとも 12 カ月に 1 回実施されていることを確認する。	
カスタマイズアプローチの目的 メディアインベントリは定期的に検証しています。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.4.6 カード会員情報を含むハードコピー資料は、業務上または法律上の理由で不要になった場合、以下のように破棄される。 • 資料は、カード会員データを再構築できないように、クロスカットでシュレッダー、焼却、またはパルプ化する • 資料は、破壊される前に安全な保管容器に保管される	**9.4.6.a** 定期的なメディア破棄ポリシーを調査し、この要件に指定されているすべての要素に従って、ビジネス上または法律上の理由で不要になったときにカード会員データの入ったハードコピーメディアを破棄する手順が定義されていることを確認する。	ハードコピー媒体に含まれる情報を廃棄する前に破壊する手順を踏まないと、悪意のある個人が廃棄された媒体から情報を取得し、データ漏洩につながる可能性があります。例えば、「ダンプスターダイビング」と呼ばれる手法で、ゴミ箱やリサイクルボックスの中から、攻撃に利用できる情報を含むハードコピーを探し出すことがあります。 そこで、廃棄予定の資料を保管する容器を保護することで、回収中に機密情報が盗み取られることを防ぎます。
	9.4.6.b プロセスを観察し、担当者にインタビューして、ハードコピー材料がカード会員データを再構築できないようにクロスカット細断、焼却、またはパルプ化されていることを確認する。	**グッドプラクティス** 細断する容器は、中身が見えないように鍵をかけるか、容器内部へのアクセスを物理的に遮断することを検討する。
カスタマイズアプローチの目的 破壊された、または破壊が保留されているメディアから、カード会員データは復元できない。	**9.4.6.c** 破棄される情報を含む資料に使用される保管容器を観察し、その容器が安全であることを確認する。	**その他の情報** *NIST Special Publication 800-88、改訂 1 版* を参照してください。*メディアのサニタイズに関するガイドラインです。*
適用性の注記 これらの要件は、業務上または法律上の理由でメディアが不要になった場合のメディア破棄に関するもので、PCI DSS 要件 3.2.1 とは別個のものである（事業体のカード会員データ保持ポリシーに従って、不要になったカード会員データを安全に削除するための要件である）。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.4.7 カード会員データの入った電子メディアは、業務上または法律上の理由で不要になった場合、以下のいずれかを通じて破棄される。 • 電子媒体を破棄する • カード会員データが復元不可能になり、再構築できなくなる	**9.4.7.a** 定期的なメディア破棄ポリシーを調査し、ビジネス上または法律上の理由で不要になった電子メディアを破棄する手順が、この要件で指定されたすべての要素に従って定義されていることを確認する。	電子メディアに含まれる情報が不要になった時点で破棄する措置を取らなかった場合、悪意のある個人が破棄されたメディアから情報を取得し、データ漏洩につながる可能性があります。例えば、「ダンプスターダイビングと呼ばれる手法で、ゴミ箱やリサイクルボックスを探し、攻撃に利用できる情報を入手することがあります。
カスタマイズアプローチの目的	**9.4.7.b** メディア破棄プロセスを観察し、担当者にインタビューして、カード会員データのある電子メディアがこの要件で指定された方法のいずれかを介して破棄されていることを確認する。	**グッドプラクティス**
消去または破壊されたメディアからカード会員データを回復することはできない。		多くの OS の削除機能では、削除したデータを復元することができるため、専用の安全な削除機能やアプリケーションを使用して、データを復元できないようにする必要があります。
適用性の注記		**例**
これらの要件は、業務上または法律上の理由でメディアが不要になった場合のメディア破棄に関するもので、PCI DSS 要件 3.2.1 とは別個のものである（事業体のカード会員データ保持ポリシーに従って、不要になったカード会員データを安全に削除するための要件である）。		電子媒体を安全に破壊する方法としては、業界で認められている安全な削除のための規格に従った安全な消去、消磁、物理的な破壊（ハードディスクの粉砕や裁断など）などがあります。
		その他の情報
		NIST Special Publication 800-88、改訂 1 を参照してください。*メディアのサニタイズに関するガイドラインです。*

要件とテスト手順		ガイダンス
9.5 POI 端末が改ざんおよび不正な置き換えから保護される。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.5.1 ペイメントカードフォームファクタとの直接的な物理的相互作用によってペイメントカードデータを取得する POI 端末は、以下を含め、改ざんや不正な置換から保護される。 • POI 端末のリストを維持する • POI 端末を定期的に検査し、改ざんまたは不正置換がないか調べる • 不審な行動に注意し、装置の改ざんや不正な代用品を報告するよう担当者を教育する	**9.5.1** 文書化されたポリシーと手順を調べ、この要件で指定されたすべての要素を含むプロセスが定義されていることを確認する。	犯罪者は、カード読取装置や端末を盗んだり、操作したりすることで、ペイメントカードデータを盗もうとします。犯罪者は、デバイスを盗むことで、デバイスに侵入する方法を学び、正規のデバイスを、カードが入力されるたびにペイメントカードデータを送信する不正なデバイスに置き換えようとすることがよくあります。 また、デバイスの外側に「スキミング」コンポーネントを追加しようとします。スキミングコンポーネントは、デバイスに入力される前にペイメントカードデータをキャプチャするように設計されています。例えば、正規のカードリーダーの上に追加のカードリーダーを取り付け、ペイメントカードのデータを犯人のコンポーネントとデバイスの正規コンポーネントで二重に取り込むようにするのです。この方法では、犯人がペイメントカードデータを「スキミング」している間でも、取引を中断することなく完了することができます。
カスタマイズアプローチの目的		**その他の情報**
事業体は、POS デバイスを保護し管理するための手順を定義している。POI 端末の管理および保護に対する期待、コントロール、および監視が定義され、影響を受ける担当者によって順守されている。		スキミング防止に関するその他のベストプラクティスは、PCI SSC の ウェブ サイトでご覧いただけます。

要件とテスト手順		ガイダンス
適用性の注記 これらの要件は、カードを提示する取引（すなわち、スワイプ、タップ、またはディップされるカードなどの支払カードのフォームファクタ）に使用される配備された POI 端末に適用される。この要件は、コンピュータのキーボードなど、手動の PAN キー入力コンポーネントに適用することを意図したものではない。 この要件は、コンピュータキーボードなどの手動 PAN キー入力コンポーネントに推奨されるが、必須ではない。 この要件は、大量販売用に設計されたモバイル機器である商用オフザシェルフ（COTS）デバイス（例えば、スマートフォンやタブレット）には適用されない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
9.5.1.1 POI 機器の最新のリストが管理されており、その内容は以下の通りである。 • 機器のメーカーとモデル • 装置の場所 • 装置の製造番号または他のユニークな識別方法	**9.5.1.1.a** POI 機器のリストを調べ、この要件で指定されたすべての要素が含まれていることを確認する。 **9.5.1.1.b** POI 端末とデバイスの位置を観察し、リスト内のデバイスと比較して、リストが正確で最新であることを確認する。 **9.5.1.1.c** POI 機器のリストが、機器の追加、移動、廃止などの際に更新されていることを確認するために、担当者にインタビューを行う。	POI 端末の最新リストを作成することは、デバイスの所在を把握し、デバイスの紛失を迅速に特定するのに役立ちます。 **グッドプラクティス** 機器一覧の管理方法は、自動化（例：機器管理システム）でも手動化（例：電子記録や紙媒体の記録）でも構いません。移動式装置の場合、装置の場所はその装置が割り当てられている関係者の名前にできます。 **例** 機器の設置場所を管理する方法として、機器が設置されているサイトまたは施設の住所により特定することができる。
カスタマイズアプローチの目的		
POI 機器の識別と位置が記録され、常に把握されていること。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** デバイスを定期的に検査することで、カードスキマーの追加やデバイスの交換などの外部証拠により改ざんをより迅速に検出し、不正なデバイスの使用による潜在的な影響を最小化することができます。 **グッドプラクティス** 定期点検の方法としては、シリアル番号など機器の特徴を確認し、POI 端末リストと照らし合わせて、不正な端末とすり替えられていないことを確認します。 **例** 検査の種類は、機器によって異なります。例えば、安全であることが分かっているデバイスの写真を使用して、デバイスの現在の外観と元の外観を比較し、変化しているかどうかを確認することができます。また、UV ライトマーカーのような安全なマーカーペンを使って、デバイスの表面や開口部にマークを付け、改ざんや交換があったことが分かるようにすることもできます。犯罪者はしばしば、デバイスの外装を交換して改ざんを隠しますが、こうした方法はそうした行為を発見するのに役立つかもしれません。また、デバイス・ベンダは、デバイスが改ざんされているかどうかを判断するためのセキュリティ *(次ページに続く)*
9.5.1.2 POI 端末の表面は定期的に検査され、改ざんや不正置換を検出すること。	**9.5.1.2.a** 文書化された手順を調べ、POI 装置表面の改ざんおよび不正置換を検出するための定期的な検査のためのプロセスが定義されていることを確認する。	
	9.5.1.2.b 担当者にインタビューし、検査工程を観察して確認する。 • 担当者は、装置を検査する手順を認識している。 • すべての装置は、改ざんおよび不正置換の証拠について定期的に検査されている。	
カスタマイズアプローチの目的		
POI 端末は、改ざんされたり、許可なく代用されたり、適時に検知されることなくスキミングのアタッチメントを取り付けられたりすることはできない。		

要件とテスト手順		ガイダンス
		ガイダンスや「ハウツー」ガイドを提供している場合があります。 デバイスが改ざんまたは置換された可能性がある兆候としては、デバイスに接続された予期せぬアタッチメントやケーブル、セキュリティ・ラベルの欠落または変更、ケースの破損、異なる色、シリアル番号やその他の外部マーキングの変更などが挙げられます。
定義されたアプローチの要件 **9.5.1.2.1** POI 端末の定期検査の頻度および実施する検査の種類は、要件 12.3.1 に規定するすべての要素に従って実施される、事業体の目標リスク分析において定義される。 **カスタマイズアプローチの目的** POI 装置は、事業体のリスクに対応した頻度で検査されている。 **適用性の注記** この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要があります。	**定義されたアプローチのテスト手順** **9.5.1.2.1.a** リスク分析が要件 12.3.1 に規定するすべての要素に従って実施されたことを確認するために、POI 端末の定期点検の頻度および実施した点検の種類に関する事業体の目標リスク分析を確認する。 **9.5.1.2.1.b** 定期的な装置検査の文書化された結果を調べ、担当者にインタビューを行い、実施された POI 端末検査の頻度と種類が、この要件のために実施した事業体の目標リスク分析で定義されたものと一致していることを確認する。	**目的** POI 端末の検査頻度は、デバイスが動作する環境に応じて、事業体が決定するのが最も適切です。 **グッドプラクティス** 点検の頻度は、機器の設置場所や有人・無人などの要因によって異なります。例えば、組織の職員による監視がなく公共の場に放置されているデバイスは、安全な場所に保管されているデバイスや一般の人がアクセスできるときに監視されているデバイスよりも、検査の頻度が高いかもしれません。さらに、多くの POI 端末ベンダは、POI 端末をどの程度の頻度で検査すべきか、また、何のために検査するかについて、POI 端末ベンダのユーザ向け文書にガイダンスを記載しています。事業体は、ベンダの文書を参照し、その推奨事項を定期点検に反映させることが推奨されます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
9.5.1.3 POI 環境にいる担当者に対して、POI 端末の改ざんや不正置換に注意するためのトレーニングが提供され、その内容は以下を含む。 • デバイスの修正またはトラブルシューティングのためのアクセスを許可する前に、修理または保守担当者であると主張する第三者の身元を確認すること • 確認なしに機器が設置、交換、返却されないようにする確実な手順を守ること • デバイス周辺での不審な行動に注意すること • 疑わしい行動、デバイスの改ざんまたは不正置換の兆候を適切な担当者に報告すること	**9.5.1.3.a** POI 環境の担当者に対する研修資料をレビューし、この要件で指定されているすべての要素が含まれていることを確認する。 **9.5.1.3.b** POI 環境の担当者にインタビューを行い、彼らがトレーニングを受け、この要件で指定されたすべての要素の手順を知っていることを確認する。	**目的** 犯罪者は、しばしば正規の保守担当者を装って POI 端末にアクセスする。 **グッドプラクティス** 代理店、保守・修理担当者、技術者、サービスプロバイダ、その他の第三者を含め、POI の保守を行うために現れた人物に注意を払い、彼らが権限を持ち、有効な作業指示書を持っているかどうかを質問することを、担当者のトレーニングに含める必要があります。例えば、管理者に確認するか、ベンダやアクワイアラーなどの POI メンテナンス会社に電話をして確認を取るなど、デバイスへのアクセスを要求する第三者はすべて、アクセスを提供される前に必ず確認する必要があります。多くの犯罪者は、工具箱を持ち、作業着に身を包むなどして、担当者の目を欺こうとします。また、デバイスの位置についても知っている可能性があるので、担当者は常に手順に従うよう訓練する必要があります。 もう一つの手口は、「新しい」POI 端末を送り、それを正規のデバイスと交換し、正規のデバイスを「返却」するよう指示することです。犯罪者は、指定された住所に返送するための郵便料金まで提供することがあります。 *(次ページに続く)*
カスタマイズアプローチの目的 担当者は、POI 端末に対する攻撃の種類、事業体の技術的・手続き的対策について知識があり、必要なときに支援や指導を受けることができる。		

要件とテスト手順		ガイダンス
		したがって、担当者は、端末を設置したり、 業務で使用する前に、必ず上司やサプライヤーに、そのデバイスが正規のものであり、信頼できる供給元から来たものであることを確認する必要があります。 **例** 担当者が注意すべき不審な行動には、未知の人物による機器の取り外しやカバーを開ける試みが含まれます。 従業員が、疑わしい行動を報告する仕組みと、そのような行動を報告する相手（例えば、管理者やセキュリティ担当者）について確実に認識することは、デバイスが改ざんされたりすり替えられたりする可能性と潜在的な影響を減らすのに役立ちます。

ネットワークの定期的な監視とテスト

要件 10 :　　システムコンポーネントおよびカード会員データへのすべてのアクセスをログに記録し、監視すること

セクション
10.1 システムコンポーネントおよびカード会員データへのすべてのアクセスをログに記録し、監視するためのプロセスおよびメカニズムが定義され、文書化されている。
10.2 異常や疑わしい活動の検出および、イベントのフォレンジック分析をサポートするために、監査ログが実装されている。
10.3 監査ログは、破壊や不正な改ざんから保護されている。
10.4 監査ログは、異常または疑わしい活動を特定するためにレビューされる。
10.5 監査ログの履歴は保持され、分析に利用できまる。
10.6 時間同期メカニズムが、すべてのシステムで一貫した時間設定をサポートしている。
10.7 重要なセキュリティ管理システムの障害を迅速に検知し、報告し、対応する。

概要

データ漏洩を防止、検出、またはその影響を最小化するためには、ログの仕組みとユーザの行動を追跡する機能が重要です。すべてのシステムコンポーネントおよびカード会員データ環境（CDE）にログが存在することで、何か問題が発生した場合に、徹底的な追跡、警告、および分析が可能になります。システムアクティビティログがなければ、侵害の原因を特定することは不可能ではないにせよ、困難です。

この要件は、従業員、請負業者、コンサルタント、社内外のベンダ、その他の第三者（例えば、サポートまたは保守サービスを提供する者）による活動を含む、ユーザの活動に適用されます。

これらの要件は、消費者（カード会員）のユーザ活動には適用されません。

PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
10.1 システムコンポーネントおよびカード会員データへのすべてのアクセスを記録および監視するためのプロセスおよびメカニズムが定義され、文書化されている。		
定義されたアプローチの要件 **10.1.1** 要件 10 で特定されたすべてのセキュリティポリシーと運用手順が • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に知られている。	**定義されたアプローチのテスト手順** **10.1.1** 文書を調査し、担当者にインタビューを行って、要件 10 で特定されたセキュリティポリシーと運用手順が、この要件で指定されたすべての要素に従って管理されていることを確認する。	**目的** 要件 10.1.1 は、要件 10 を通して指定された様々なポリシーと手順を効果的に管理および維持することに関するものです。要件 10 で言及されている特定のポリシーや手順を定義することは重要であるが、それらが適切に文書化され、維持され、普及していることを確認することも同様に重要です。 **グッドプラクティス** プロセス、技術、ビジネス目的の変化に対応するため、ポリシーと手順を必要に応じて更新することが重要です。そのため、定期的な更新だけでなく、変更が発生したらできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、企業のセキュリティの目的および原則を定義します。運用手順は、活動の方法を説明し、一貫した方法で、かつ、ポリシーの目的に沿って望ましい結果を達成するために従う統制、方法、プロセスを定義しています。
カスタマイズアプローチの目的 要件 10 内の活動を満たすための期待、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべての支援活動が繰り返し可能であり、一貫して適用され、経営者の意図に適合している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要な活動が行われない可能性があります。 **グッドプラクティス** 役割と責任は、ポリシーと手順の中で文書化されるか、または別の文書で管理されるかもしれません。 役割と責任を伝える一環として、事業体は、担当者に与えられた役割と責任を受け入れ、理解することに同意してもらうことを検討することができます。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担マトリックス（RACI マトリックスとも呼ばれます） があります。
10.1.2 要件 10 の活動を行うための役割と責任が文書化され、割り当てられ、理解されている。	**10.1.2.a** 文書を調査し、要件 10 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	10.1.2.b 要件 10 の活動実施に責任を持つ担当者にインタビューを行い、役割と責任が定義通りに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 10 のすべての活動を実行するための日々の責任が割り当てられている。担当者は、これらの要件の成功、継続的な運用に責任を負う。		

要件とテスト手順		ガイダンス
10.2 監査ログが実装され、異常や疑わしい活動の検出、およびイベントのフォレンジック分析がサポートされる。		
定義されたアプローチの要件 **10.2.1** 監査ログは、すべてのシステムコンポーネントおよびカード会員データに対して有効であり、アクティブである。	**定義されたアプローチのテスト手順** **10.2.1** システム管理者にインタビューを行い、システム構成を調査し、すべてのシステムコンポーネントに対して監査ログが有効であり、アクティブであることを確認する。	**目的** すべてのシステムコンポーネントについてログが存在していなければなりません。監査ログは、システム管理者にアラートを送信し、侵入検知システム（IDS）やセキュリティ情報およびイベント監視システム（SIEM）ツールなどの他の監視メカニズムにデータを提供し、インシデント後の調査のための履歴証跡を提供します。 セキュリティ関連のイベントをログに記録し、分析することで、組織は潜在的に悪意のある活動を特定し、追跡することができます。 **グッドプラクティス** 事業体がログに記録する情報を検討する場合、監査ログに保存される情報は機密情報であり、本標準の要件に従って保護されるべきであることを忘れないようにすることが重要です。リスクを最小化するために、監査ログには必要不可欠な情報のみを保存するよう注意すべきです。
カスタマイズアプローチの目的 システムコンポーネントおよびカード会員データに影響するすべての活動の記録が取得される。		
定義されたアプローチの要件 **10.2.1.1** 監査ログで、カード会員データへのすべての個々のユーザクセスを記録する。	**定義されたアプローチのテスト手順** **10.2.1.1** 監査ログの構成およびログデータを調査し、カード会員データへの個々のユーザのアクセスがすべてログ に記録されていることを確認する。	**目的** ユーザクセスとアクセスしたシステムコンポーネントを関連付けるプロセスまたはシステムを持つことが重要です。 *(次ページに続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 カード会員データへのすべての個々のユーザクセスの記録が取得される。		悪意のある個人が、カード会員データ環（CDE）内のシステムにアクセスできるユーザカウントの知識を得たり、カード会員データにアクセスするために新しい未承認のアカウントを作成したりする可能性があります。 **グッドプラクティス** カード会員データへの個々の全アクセスを記録することで、どのアカウントが漏洩または不正使用された可能性が あるかを特定することができます。
定義されたアプローチの要件 **10.2.1.2** 監査ログには、アプリケーションまたはシステムアカウントの対話的な使用を含め、管理アクセスを持つ個人が行ったすべてのアクションが記録される。 **カスタマイズアプローチの目的** 昇格した権限を持つ個人が実行したすべてのアクションの記録が取得されている。	**定義されたアプローチのテスト手順** **10.2.1.2** 監査ログの設定およびログデータを調査し、アプリケーションまたはシステムアカウントの対話的な使用を含む管理アクセス権を有する個人によって実行されたすべてのアクションがログに記録されていることを確認する。	**目的** 「管理者」や「ルート」アカウントなど、アクセス権限の高いアカウントは、システムのセキュリティや運用機能に大きな影響を与える可能性があります。実行された活動のログがなければ、組織は、管理上のミスや特権の誤用に起因する問題を、特定の行為やアカウントに遡って追跡することができません。 **定義** 管理者アクセス権を持つアカウントとは、システム、ネットワーク、および／またはアプリケーションを管理するための、特定の特権または能力を割り当てられているアカウントです。管理用とみなされる機能または活動は、通常の業務機能の一部として一般のユーザが実行するものを超えるものです。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **10.2.1.3** 監査ログは監査ログへのすべてのアクセスを取得する。 **カスタマイズアプローチの目的** 監査ログへのすべてのアクセスの記録が取得されていること。	**定義されたアプローチのテスト手順** **10.2.1.3** 監査ログの設定とログデータを調査し、すべての監査ログへのアクセスが取得されていることを確認する。	**目的** 悪意のあるユーザは、しばしば自分の行動を隠すために監査ログを改ざんしようとします。アクセスの記録により、組織はログの不整合や改ざんの可能性を、個人アカウントまで追跡することができます。監査ログの変更、追加、削除を特定するログを持つことで、無許可の者が取ったステップを追跡するのに役立ちます。
定義されたアプローチの要件 **10.2.1.4** 監査ログは、すべての無効な論理的アクセスの試行を記録する。 **カスタマイズアプローチの目的** すべての無効なアクセスの試行の記録が取得されている。	**定義されたアプローチのテスト手順** **10.2.1.4** 監査ログの設定とログデータを調査し、無効な論理敵アクセスの試行が取得されていることを確認する。	**目的** 悪意のある人物は、しばしば標的のシステムに対して何度もアクセスを試みます。複数の無効なログイン試行は、不正なユーザがパスワードを「ブルートフォース」または推測しようとしたことを示す可能性があります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **10.2.1.5** 監査ログは、以下のような識別情報および認証情報へのすべての変更を記録する。 • 新しいアカウントの作成 • 特権の昇格 • 管理者アクセス権を持つアカウントに対するすべての変更、追加、または削除 **カスタマイズアプローチの目的** 識別情報および認証情報に対するすべての変更記録が取得されている。	**定義されたアプローチのテスト手順** **10.2.1.5** 監査ログの構成およびログデータを調べ、識別情報および認証情報への変更がこの要件で指定されたすべての要素に従って取得されていることを確認する。	**目的** 認証情報の変更（特権の昇格、追加、管理者権限を持つアカウントの削除を含む）を記録することで、活動の残存証拠を得ることができます。 悪意のあるユーザは、認証情報を操作して迂回したり、有効なアカウントになりすましたりしようとする可能性があります。
定義されたアプローチの要件 **10.2.1.6** 監査ログは、以下を取得する。 • 新しい監査ログのすべての初期化、および • 既存の監査ログのすべての開始、停止、または一時停止 **カスタマイズアプローチの目的** 監査ログの活動状況に対するすべての変更の記録が取得されていること。	**定義されたアプローチのテスト手順** **10.2.1.6** 監査ログの構成とログデータを調査し、この要件で指定されたすべての要素が取得されていることを確認する。	**目的** 不正な活動を行う前に監査ログをオフにしたり、一時停止したりすることは、検知を避けたい悪意のあるユーザにとって一般的な行為です。監査ログが初期化されることは、ユーザが自分の行動を隠すためにログ機能を無効化したことを示す可能性があります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **10.2.1.7** 監査ログは、システムレベルオブジェクトのすべての作成と削除を記録する。 **カスタマイズアプローチの目的** システムが意図した機能から変更されたことを示す改変の記録を取得する。	**定義されたアプローチのテスト手順** **10.2.1.7** 監査ログの構成とログデータを調査し、システムレベルオブジェクトの作成と削除が取得されていることを確認する。	**目的** マルウェアなどの悪意のあるソフトウェアは、しばしばターゲットシステム上にシステムレベルオブジェクトを作成または置換し、そのシステム上の特定の機能または操作を制御します。システムレベルオブジェクトが作成または削除されたときにログを取ることで、そのような変更が許可されたかどうかを判断することが容易になります。
定義されたアプローチの要件 **10.2.2** 監査ログでは、監査可能イベントごとに次の詳細を記録します。 • ユーザの識別 • イベントの種類 • 日付と時間 • 成功および失敗の表示 • イベントの発生元 • 影響を受けるデータ、システムコンポーネント、リソース、またはサービスの識別または名前（例えば、名前とプロトコル） **カスタマイズアプローチの目的** 要件 10.2.1 に記載されている各イベントについて、成功した試行と失敗した試行や、誰が、何を、いつ、どこで、どのように行ったかを特定できる十分なデータを取得する。	**定義されたアプローチのテスト手順** **10.2.2** 担当者にインタビューを行い、監査ログ構成を調査し、この要件で指定されたすべての要素が、各監査対象イベント（10.2.1.1 から 10.2.1.7 まで）のログエントリに含まれていることを確認する。	**目的** 10.2.1.1 から 10.2.1.7 の監査対象イベントについてこれらの詳細を記録することで、潜在的な侵害を迅速に特定し、疑わしい活動のフォローアップを容易にするための十分な詳細を記録することができます。

要件とテスト手順		ガイダンス
10.3 監査ログが破壊や不正な改ざんから保護されていること。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 監査ログファイルには機密情報が含まれており、ログファイルへの読み取りアクセスは、正当な業務上の必要性を有する者のみに制限されなければなりません。このアクセスには、起点となるシステム上の監査ログファイルだけでなく、それらが保存されている他のあらゆる場所が含まれます。 **グッドプラクティス** 監査ログの適切な保護には、ログへのアクセスを「業務上必要な範囲」に基づいて制限する強力なアクセス制御と、ログを検索および変更しにくくするための物理的またはネットワーク分離の使用が含まれます。
10.3.1 監査ログファイルへの読み取りアクセスは、業務上必要な者に限定される。 **カスタマイズアプローチの目的** 保存された活動記録は、権限のない担当者がアクセスすることはできない。	**10.3.1** システム管理者にインタビューを行い、システムの設定と権限を調査し、業務上必要な個人のみが監査ログファイルへの読み取りアクセス権を持っていることを確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **10.3.2** 監査ログファイルは、個人による改ざんを防ぐために保護されている。 **カスタマイズアプローチの目的** 保存された活動記録は、担当者が変更することができない。	**定義されたアプローチのテスト手順** **10.3.2** システム構成と権限を調査し、システム管理者にインタビューを行い、現在の監査ログファイルがアクセス制御メカニズム、物理的な分離、および／またはネットワーク分離によって、個人による改ざんから保護されていることを確認する。	**目的** ネットワークに侵入した悪意のある個人が、自分の行動を隠すために監査ログを編集しようとすることがよくあります。監査ログを適切に保護しなければ、監査ログの完全性、正確性、完全性が保証されず、侵害後の調査ツールとして使えなくなる可能性があります。したがって、監査ログは、発信元のシステムだけでなく、保存されている他の場所でも保護する必要があります。 **グッドプラクティス** 事業体は、ログが一般にアクセス可能な場所にさらされることを防ぐよう努めるべきです。
定義されたアプローチの要件 **10.3.3** 監査ログファイルは、外部に公開されているテクノロジのものも含め、安全で一元的な内部ログサーバまたは変更が困難な他の媒体に速やかにバックアップされる。 **カスタマイズアプローチの目的** 保存された活動記録は、不正な改変が行われないように一元的な場所で保護され保存されている。	**定義されたアプローチのテスト手順** **10.3.3** バックアップの設定やログファイルを調査し、外部向け技術を含む現在の監査ログファイルが、安全で一元的な内部ログサーバまたは変更が困難な他の媒体に速やかにバックアップされていることを確認する。	**目的** ログを生成するシステムが侵害された場合でも、ログを一元管理したサーバや改ざん困難なメディアに速やかにバックアップすることで、ログを保護することができます。 ワイヤレス、ネットワークセキュリティ制御、DNS、メールサーバなど、外部向けの技術からログを書き出すことで、これらのログが失われたり、改ざんされたりするリスクを低減することができます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		グッドプラクティス ログファイルのバックアップは、1つまたは複数の一元管理したログサーバ、またはその他の安全なメディアを経由して行うか、各事業体が最適な方法を決定します。ログは、外部システムから安全な内部システムまたは媒体に直接書き込む、オフロードする、またはコピーすることができます。
定義されたアプローチの要件 **10.3.4** 監査ログに対してファイルの整合性監視または変更検出メカニズムを使用して、既存のログデータを変更すると警告が生成されるようにする。 **カスタマイズアプローチの目的** 保存された活動記録は、変更すると警告が生成される。	**定義されたアプローチのテスト手順** **10.3.4** システム設定、監視対象ファイル、監視活動の結果を調査し、監査ログにファイル整合性監視または変更検出ソフトウェアが使用されていることを確認する	**目的** ファイル整合性監視システムまたは変更検出システムは、重要なファイルの変更をチェックし、そのような変更が確認されたときに通知します。ファイルの整合性監視の目的で、事業体は、通常定期的に変更されないが、変更された場合、侵害の可能性を示すファイルを監視します。 **グッドプラクティス** 監査ログの変更を監視するソフトウェアは、既存のログデータまたはファイルが変更または削除されたときに警告を発するように設定する必要があります。しかし、監査ログに追加される新しいログデータは、警告を生成すべきではありません。

要件とテスト手順		ガイダンス
10.4 監査ログをレビューし、異常または疑わしいアクティビティを識別することができる。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
10.4.1 以下の監査ログを少なくとも毎日一度レビューしている。 • すべてのセキュリティイベント • カード会員データ（CHD）および／または機密認証データ（SAD）を保存、処理、または伝送するすべてのシステムコンポーネントのログ • すべての重要なシステムコンポーネントのログ • セキュリティ機能（例えば、ネットワーク・セキュリティ・コントロール、侵入検知システム／侵入防止システム（IDS／IPS）、認証サーバ）を実行するすべてのサーバおよびシステムコンポーネントのログ	**10.4.1.a** セキュリティポリシーと手順を調べ、この要件で指定されたすべての要素を少なくとも毎日一度レビューするためのプロセスが定義されていることを確認する。 **10.4.1.b** プロセスを観察し、担当者にインタビューして、この要件で指定されているすべての要素が少なくとも毎日一度レビューされていることを確認する。	多くの違反は、発見される数カ月前に発生する。定期的なログレビューにより、インシデントを迅速に特定し、積極的に対処することができます。 **グッドプラクティス** 毎日（週 7 日、1 年 365 日、休日を含む）ログを確認することで、侵害の可能性が明らかになるまでの時間と露出を最小限に抑えることができます。ログ収集・解析・警告ツール、ログ一元管理システム、イベントログ解析ツール、セキュリティ情報イベント管理（SIEM）ソリューションなどは、この要件を満たすために使用できる自動化ツールの一例です。 疑わしいまたは異常な活動を特定する通知や警告などのセキュリティイベント、重要なシステムコンポーネントからのログ、ファイアウォール、IDS／IPS、ファイル整合性監視（FIM）システムなどのセキュリティ機能を果たすシステムからのログを日々確認し、潜在的な問題を特定することが必要です。 *(次ページに続く)*
カスタマイズアプローチの目的		
潜在的に疑わしいまたは異常な活動を迅速に特定し、影響を最小限に抑える。		

要件とテスト手順		ガイダンス
		「セキュリティ・イベント」の判断は組織ごとに異なり、技術の種類、場所、装置の機能などを考慮する必要があります。また、組織は、異常な動作を特定するために、「正常な」トラフィックの基準値を維持することを望むかもしれません。 サードパーティサービスプロバイダを使用してログレビューサービスを行う事業体は、サービスプロバイダに事業体の環境に関する背景を提供する責任があります。これにより、サービスプロバイダは事業体の環境を理解し、事業体の「正常な」トラフィックのベースラインを持ち、潜在するセキュリティ問題を検出して正確な例外事象および異常通知を提供できます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **10.4.1.1** 監査ログのレビューを行うために、自動化されたメカニズムが使用されている。 **カスタマイズアプローチの目的** 潜在的に疑わしい、または異常な活動は、反復可能で一貫したメカニズムによって識別される。 **適用性の注記** この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。	**定義されたアプローチのテスト手順** **10.4.1.1** ログレビューのメカニズムを調べ、担当者にインタビューし、自動化されたメカニズムでログレビューが実施されていることを確認する。	**目的** ログデータの量が多いため、1〜2 システムであっても手動でログレビューを行うことは困難です。しかし、ログ収集・解析・警告ツール、ログ一元管理システム、イベントログ解析ツール、セキュリティ情報イベント管理（SIEM）ソリューションを使用すれば、レビューが必要なログイベントを特定し、プロセスを円滑にすることができます。 **グッドプラクティス** 事業体は、定期的にツールの設定を確認し、変更を反映するために設定を更新することにより、ロギングツールを環境の変更に対応させる必要があります。
定義されたアプローチの要件 **10.4.2** その他全てのシステムコンポーネント（要件 10.4.1 に規定しないもの）のログを定期的にレビューする。 *(次ページに続く)*	**定義されたアプローチのテスト手順** **10.4.2.a** セキュリティポリシーおよび手順を調査し、他のすべてのシステムコンポーネントのログを定期的にレビューするためのプロセスが定義されていることを確認する。 **10.4.2.b** ログレビューの文書化された結果を調査し、担当者にインタビューすることで、ログレビューが定期的に実施されていることを確認する。	**目的** 他のすべてのシステムコンポーネント（要件 10.4.1 に規定されていない）のログを定期的にレビューすることで、潜在的な問題や重要度の低いシステムを経由して重要なシステムにアクセスしようとする兆候を特定することができます。

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 他のシステムコンポーネント（10.4.1 に含まれない）について、潜在的に疑わしいまたは異常な活動を、事業体が識別したリスクに従ってレビューする。 **適用性の注記** この要件は、要件 10.4.1 に含まれない他のすべての適用範囲のシステムコンポーネントに適用される。		
定義されたアプローチの要件 **10.4.2.1** その他のシステムコンポーネント（要件 10.4.1 で定義されていないもの）に対する定期的なログレビューの頻度は、要件 12.3.1 で指定されたすべての要素に従って実行される事業体のターゲットリスク分析で定義される。 **カスタマイズアプローチの目的** 低リスクのシステムコンポーネントのログレビューが、事業体のリスクに対応した頻度で実施されている。	**定義されたアプローチのテスト手順** **10.4.2.1.a** その他のシステムコンポーネント（要件 10.4.1 に定義されていない）の定期的なログレビューの頻度について、事業体のターゲットリスク分析を調べ、要件 12.3.1 で指定されたすべての要素に従ってリスク分析 が実施されたことを確認する。 **10.4.2.1.b** 他のすべてのシステムコンポーネント（要件 10.4.1 に定義されていない）の定期的なログレビューの文書化された結果を調べ、担当者にインタビューして、 *(次ページに続く)*	**目的** 事業体は、各事業体の環境の複雑さ、評価が必要なシステムの種類数、および当該システムの機能などの基準に基づいて、これらのログをレビューする最適な期間を決定することができます。

要件とテスト手順		ガイダンス
適用性の注記 この要件は 2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。	ログレビューがこの要件のために実施された事業体のターゲットリスク分析で 指定された頻度で実施されていることを確認する。	
定義されたアプローチの要件 **10.4.3** レビューの過程で確認された例外や異常に対処している。	**定義されたアプローチのテスト手順** **10.4.3.a** セキュリティポリシーと手順を調べ、レビュープロセスで特定された例外と異常に対処するためのプロセスが定義されていることを確認する。	**目的** ログレビューの過程で特定された例外や異常を調査しない場合、事業体はネットワーク内で発生している不正な活動や悪意のある可能性のある活動に気づかない可能性があります。 **グッドプラクティス** 事業体は、例外や異常を定義し、管理するプロセスを開発する際に、以下の点にどのように対処するかを検討する必要があります。 • ログレビュー活動の記録方法 • 例外や異常のランク付けと優先順位付けの方法 • 例外や異常を報告し、エスカレーションするために、どのような手順を踏むべきか • 調査および修正作業の責任者は誰か
カスタマイズアプローチの目的 疑わしい活動や異常な活動に対処している。	**10.4.3.b** プロセスを観察し、担当者にインタビューし、例外や異常が特定された場合、それらに対処していることを確認する。	

要件とテスト手順		ガイダンス
10.5 監査ログの履歴を保持し、分析に利用できるようにしている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**グッドプラクティス**
10.5.1 監査ログの履歴を少なくとも 12 カ月間保持し、少なくとも直近の 3 カ月間は分析のために直ちに利用できるようにする。	**10.5.1.a** 以下のことが定義されていることを確認するために、文書を調査する。 • 監査ログの保持方針 • 監査ログの履歴を少なくとも 12 カ月間保持し、少なくとも直近の 3 カ月間はオンラインで直ちに利用できるようにするための手順	侵害はかなりの期間気付かれないことが多いため、少なくとも 12 カ月間は監査ログを履歴として保持することが必要です。ログ履歴を一元的に保管することで、調査員は、潜在的な侵害が発生していた期間と、影響を受けた可能性のあるシステムをより適切に判断することができます。3 カ月分のログをすぐに利用できるようにすることで、事業体はデータ侵害を迅速に特定し、その影響を最小限に抑えることができます。
	10.5.1.b 監査ログの履歴の構成を調べ、担当者にインタビューし、監査ログを調査して、監査ログの履歴が少なくとも 12 カ月間保持されていることを確認する。	**例** ログをすぐに利用できる方法としては、ログをオンラインで保存する、ログをアーカイブする、バックアップからログを迅速に復元するなどがあります。
カスタマイズアプローチの目的	**10.5.1.c** 担当者にインタビューし、プロセスを観察して、少なくとも直近の 3 カ月間の監査ログ履歴が直ちに分析に利用できることを確認する。	
活動の履歴記録がインシデント対応を支援するために直ちに利用可能であり、少なくとも 12 カ月間保持されている。		

要件とテスト手順		ガイダンス
10.6 時刻同期メカニズムが、すべてのシステムで一貫した時刻設定をサポートすること		
定義されたアプローチの要件 **10.6.1** 時刻同期技術により、システムクロックおよび時刻を同期させる。 **カスタマイズアプローチの目的** すべてのシステムで共通の時刻が設定されている。 **適用上の注意** 時刻同期技術を最新の状態に保つには、PCI DSS 要件 6.3.1 および 6.3.3 に従って脆弱性を管理し、技術にパッチを適用することが含まれます。	**定義されたアプローチのテスト手順** **10.6.1** システム構成の設定を調査し、時刻同期技術が実装され、最新の状態に保たれていることを確認する。	**目的** 時刻同期技術は、複数のシステムのクロックを同期するために使用されます。クロックが正しく同期されていない場合、異なるシステムのログファイルを比較し、侵害に沿ったフォレンジック分析のために重要であるイベントの正確な順序を確立することは不可能ではないにしても、困難となる可能性があります。 インシデント後のフォレンジックチームにとって、すべてのシステムクロックの正確さと一貫性、および各アクティビティの時刻は、システムがどのように侵害されたかを判断する上で非常に重要です。 **例** 時刻同期技術の一例として、NTP（ネットワークタイムプロトコル）があります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
10.6.2 システムは次のように正しく一貫した時刻に設定されている。 • 1 つ以上の指定したタイムサーバが使用されている。 • 指定した中央タイムサーバだけが外部ソースから時刻を受信する。 • 外部ソースから受信した時刻は、国際原子時または協定世界時（UTC）に基づく。 • 指定したタイムサーバは、業界で認められた特定の外部ソースからの時間更新のみを受け入れる。 • 複数の指定したタイムサーバがある場合、タイムサーバは正確な時間を保つために互いにピアリングを行う。 • 内部システムは、指定した中央タイムサーバからのみ時間情報を受信する。	**10.6.2** 正しい時刻を取得、配布、保存するためのシステム構成設定を調べ、設定がこの要件で指定されたすべての要素に従って構成されていることを確認する。	**目的** 信頼できるタイムサーバを使用することは、時刻同期のプロセスにおいて重要な要素です。 業界で認められている特定の外部ソースからの時刻更新を受け入れることで、悪意のある個人がシステムの時刻設定を変更することを防ぐことができます。 **グッドプラクティス** 内部タイムサーバの不正使用を防ぐには、更新を対称鍵で暗号化し、時刻更新が提供されるクライアントマシンの IP アドレスを指定するアクセス制御リストを作成する方法もあります。
カスタマイズアプローチの目的 すべてのシステムの時刻は正確で一貫している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
10.6.3 時刻同期の設定とデータは、以下のように保護されていする。 • 時刻データへのアクセスは、業務上必要な担当者のみに制限される。 • 重要なシステムの時刻設定の変更は、ログに記録され、監視され、レビューされる。	**10.6.3.a** システム構成と時間同期設定を調査し、時間時刻データへのアクセスが業務上必要な担当者にのみ制限されていることを確認する。	攻撃者は自分の活動を隠すために、時刻の設定を変更しようとします。そのため、時刻同期設定やシステム時刻を変更・修正する権限を管理者に限定することで、攻撃者が時刻設定の変更に成功する確率を低くすることができます。
カスタマイズアプローチの目的	**10.6.3.b** システム構成、時刻同期設定、ログを調査し、プロセスを観察して、重要なシステムの時刻設定のあらゆる変更がログに記録され、監視され、レビューされていることを確認する。	
システムの時刻設定は、権限のない担当者によって変更されない。		

要件とテスト手順		ガイダンス
10.7 重要なセキュリティ管理システムの障害を迅速に検知し、報告し、対応する。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
10.7.1 ***サービスプロバイダのための追加要件：***、重要なセキュリティ管理システムの障害を迅速に検知し、警告し、対処すること。以下の重要なセキュリティ対策システムの障害を含むが、これらに限定されない： • ネットワークセキュリティ管理 • IDS／IPS • FIM • マルウェア対策ソリューション • 物理アクセス制御 • 論理アクセス制御 • 監査ログメカニズム • セグメンテーション制御（使用している場合）	**10.7.1.a** ***サービスプロバイダ評価のみの追加テスト手順：***重要なセキュリティ制御システムの障害を迅速に検知し、対処するためのプロセスが定義されていることを検証するために、文書を調査する。障害には、この要件で指定されたすべての要素の障害を含むが、これらに限定されない。	重要なセキュリティ対策の障害を検知し警告する正式なプロセスがない場合、障害が長期間検知されず、攻撃者がシステムコンポーネントに侵入し、カード会員データ環境（CDE）からアカウントデータを盗むのに十分な時間を提供する可能性があります。
カスタマイズアプローチの目的	**10.7.1.b** ***サービスプロバイダ評価のみの追加試験手順。***重要なセキュリティ管理システムの障害が検知・報告されていること、および重要なセキュリティ管理システムの障害が警告の発生につながることを検証するために、検知・警告プロセスを観察し、担当者にインタビューする。	**グッドプラクティス**
重要なセキュリティ制御システムの障害が迅速に特定され、対処されている。		具体的な障害の種類は、機器システムのコンポーネントの機能や使用されている技術によって異なる場合があります。典型的な障害は、システムがセキュリティ機能を果たさなくなること、例えばファイアウォールがそのルールをすべて消去するかオフラインになるなど、意図した方法で機能しなくなることを含みます。

要件とテスト手順		ガイダンス
適用上の注意 この要件は、評価対象組織がサービスプロバイダである場合にのみ適用される。 この要件は、2025 年 3 月 31 日をもって要件 10.7.2 に置き換わる予定です。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 重要なセキュリティ対策の障害を検知し警告する正式なプロセスがない場合、障害が長期間検知されず、攻撃者にシステムコンポーネントを危険にさらし、カード会員データ環境（CDE）からアカウントデータを盗むのに十分な時間を提供する可能性があります。 **グッドプラクティス** 具体的な障害の種類は、機器システムのコンポーネントの機能や使用されている技術によって異なる場合があります。しかし、典型的な障害には、システムがセキュリティ機能を果たさなくなる、または意図した方法で機能しなくなること、例えば、ファイアウォールがルールを消去したりオフラインになったりすることが含まれます。
10.7.2 重要なセキュリティ対策システムの障害が迅速に検知され、警告され、対処される。（以下の重要なセキュリティ制御システムの障害に限定されない。） • ネットワークセキュリティ制御 • IDS／IPS • 変更検出メカニズム • マルウェア対策ソリューション • 物理アクセス制御 • 論理アクセス制御 • 監査ログメカニズム • セグメンテーション制御（使用している場合） • 監査ログレビューメカニズム • 自動化されたセキュリティテストツール（使用している場合）	**10.7.2.a** 文書を調査して、重要なセキュリティ対策システムの障害を迅速に検出し、対処するためのプロセスが定義されていることを確認する。障害には、この要件で指定されたすべての要素の障害を含むが、これらに限定されない。 **10.7.2.b** 重要なセキュリティ管理システムの障害が検知・報告されていること、および重要なセキュリティ管理システムの障害が警告の発生につながることを確認するため、検知・警告プロセスを観察し、担当者にインタビューする。	

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 重要なセキュリティ管理システムの障害が迅速に特定され、対処されている。		
適用上の注意 この要件は、サービスプロバイダを含むすべての事業者に適用され、2025 年 3 月 31 日に要件 10.7.1 に取って代わられる予定である。要件 10.7.1 にはない 2 つの重要なセキュリティ管理システムが追加されている。 この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
10.7.3 重要なセキュリティ対策システムの障害には、迅速な対応を行う。対応には以下を含むがこれらに限定されない： • セキュリティ機能を復旧させる。 • セキュリティ障害の発生期間（発生から終了までの日時）を特定し、文書化する。 • 障害の原因を特定、文書化し、必要な是正措置を文書化する。 • 障害発生時に起きたセキュリティ上の問題を特定し、対処する。 • セキュリティ障害の結果、さらなる対策が必要であるかどうかを判断する。 • 障害原因の再発を防止するための対策を実施する。 • セキュリティ対策の監視を再開する。	**10.7.3.a** 文書を調査し、担当者にインタビューをして、重要なセキュリティ対策システムの障害に対応するためのプロセスが定義、実施されており、少なくともこの要件で指定されたすべての要素が含まれていることを確認する。	**目的** 重要なセキュリティ対策システムの障害による警告に迅速かつ効果的に対応しない場合、攻撃者はこの時間を利用して悪意のあるソフトウェアを挿入し、システムを制御したり、事業体の環境からデータを盗んだりする可能性があります。 **グッドプラクティス** 文書化された証跡（例えば、問題管理システム内の記録）は、セキュリティ障害に対応するためのプロセスおよび手順が整備されていることの裏付けとなるべきです。さらに、担当者は、障害が発生した場合の責任を認識していなければなりません。障害に対する措置および対応は、文書化された証拠として収集するべきです。
カスタマイズアプローチの目的 重要なセキュリティ対策システムの障害を分析、抑制、解決し、影響を最小化するためにセキュリティ対策を復旧させる。その結果キュリティ上の問題は対処され、再発防止策が講じられる。 *(次ページに続く)*	**10.7.3.b** 記録を調査して、重要なセキュリティ対策システムの障害が以下を含むように文書化されていることを確認する。 • 障害の原因を特定する。 • セキュリティ障害の期間（開始と終了の日付と時間）。 • 根本原因に対処するために必要な是正措置の詳細。	

要件とテスト手順		ガイダンス
適用上の注意 この要求事項は、評価対象企業がサービス提供者である場合にのみ、2025 年 3 月 31 日まで適用され、それ以降はすべての企業に適用されます。 *これは、サービスプロバイダにのみ適用される現在の v3.2.1 の要件である。ただし、この要件は 2025 年 3 月 31 日まではその他のすべての事業体のベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に考慮する必要がある。*		

要件 11 :　　システムおよびネットワークのセキュリティを定期的にテストする

セクション
11.1 システムおよびネットワークのセキュリティを定期的にテストするためのプロセスおよび仕組みが定義され、理解されている。
11.2 ワイヤレスアクセスポイントを特定、監視し、不正なワイヤレスアクセスポイントに対処している。
11.3 外部および内部の脆弱性を定期的に特定し、優先順位をつけ、対処している。
11.4 外部および内部へのペネトレーションテストを定期的に実施し、悪用可能な脆弱性およびセキュリティ上の弱点を是正している。
11.5 ネットワークへの侵入や予期せぬファイルの変更を検知し、対処している。
11.6 決済ページの不正な改変を検知し、対応している。

概要

脆弱性は、悪意のある人物や研究者によって絶えず発見されたり、新しいソフトウェアから取り込まれています。システムコンポーネント、プロセス、特注およびカスタムソフトウェアは、変化する環境を反映したセキュリティ制御が継続できるよう、頻繁にテストする必要があります。

PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
11.1 システムおよびネットワークのセキュリティを定期的にテストするためのプロセスおよび仕組みが定義され、理解されている。		
定義されたアプローチの要件 **11.1.1** 要件 11 で特定されたすべてのセキュリティポリシーと運用手順が、 • 文書化されている。 • 最新の状態に保たれている。 • 使用されている。 • すべての関係者に知られている。 **カスタマイズアプローチの目的** 要件 11 内の活動を満たすための期待、制御、および監視が定義され、影響を受ける担当者によって順守されている。すべての支援活動が繰り返し可能であり、一貫して適用され、経営者の意図に適合している。	**定義されたアプローチのテスト手順** **11.1.1** 文書を調査し、担当者にインタビューして、セキュリティポリシーと運用手順がこの要件で指定されているすべての要素に従って管理されていることを確認する。	**目的** 要件 11.1.1 の目的は、要件 11 を通して指定された様々なポリシーと手順を効果的に管理し、維持することです。要件 11 に記載される特定のポリシーや手順を定義することは重要ですが、それらが適切に文書化され、維持され、普及することを保証することも同様に重要です。 **グッドプラクティス** プロセス、技術、ビジネス目的の変化に対応するために、ポリシーと手順を必要に応じて更新することが重要です。このため、定期的な更新だけでなく、変更があった場合はできるだけ早く更新することを検討します。 **定義** セキュリティポリシーは、事業体のセキュリティの目的および原則を定義するものです。運用手順は、活動の実行方法を記述し、一貫した方法で、ポリシーの目標に従って望ましい結果を達成するために従う統制、方法、プロセスを定義します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 役割と責任が正式に割り当てられていない場合、担当者は日々の責任を認識できず、重要な活動が行われない可能性があります。 **グッドプラクティス** 役割と責任は、ポリシーと手順の中で文書化されるか、または別の文書で管理されるかもしれません。 役割と責任を伝える一環として、事業体は、担当者に与えられた役割と責任を受け入れ、理解することに同意してもらうことを検討することができます。 **例** 役割と責任を文書化する方法として、実行責任者、説明責任者、協業先、報告先を含む責任分担マトリックス（RACI マトリックスとも呼ばれる）があります。
11.1.2 要件 11 の活動を実施するための役割と責任が文書化され、割り当てられ、理解されている。	**11.1.2.a** 文書を調査して、要件 11 の活動を行うための役割と責任に関する記述が文書化され、割り当てられていることを確認する。	
	11.1.2.b 要件 11 の活動の実施に責任を持つ担当者にインタビューを行い、役割と責任が文書化されたとおりに割り当てられ、理解されていることを確認する。	
カスタマイズアプローチの目的		
要件 11 のすべての活動を実施するための日常的な責任が割り当てられている。担当者は、これらの要件の正常かつ継続的な運用に責任を持つ。		

要件とテスト手順		ガイダンス
11.2 ワイヤレスアクセスポイントを特定、監視し、不正なワイヤレスアクセスポイントに対処している。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.2.1 承認されたワイヤレスアクセスポイントおよび許可されていないワイヤレスアクセスポイントは、以下のように管理さる。 • ワイヤレス（Wi-Fi）アクセスポイントの存在が検査される。 • すべての承認されたワイヤレスアクセスポイントおよび承認されていないワイヤレスアクセスポイントが検出され、識別される。 • テスト、検出、識別は少なくとも 3 カ月に 1 回行われる。 • 自動監視を使用する場合は、生成されたアラートを介して担当者に通知す。	**11.2.1.a** ポリシーと手順を調べ、この要件で指定されたすべての要素を持つ承認されたワイヤレスアクセスポイントおよび承認されていないワイヤレスアクセスポイントの両方を管理するためのプロセスが定義されていることを確認する。 **11.2.1.b** 使用している手法および結果の文書を調査し、担当者にインタビューして、この要件で指定されたすべての要素に従って、承認されたワイヤレスアクセスポイントおよび承認されていないワイヤレスアクセスポイントの両方を検出および識別するためのプロセスが定義されていることを確認する。 **11.2.1.c** ワイヤレス評価結果を調べ、担当者にインタビューして、この要件で指定されたすべての要素に従ってワイヤレス評価が実施されたことを確認する。 **11.2.1.d** 自動監視を使用している場合、構成設定を調べ、担当者に通知するための警告を生成する構成を確認する。	ネットワーク内でのワイヤレステクノロジの実装および／または悪用は、悪意のあるユーザがネットワークおよびカード会員データに不正にアクセスするための一般的な経路です。不正なワイヤレスデバイスは、コンピュータまたは他のシステムコンポーネントの中に隠されているか、またはそれらに取り付けられている可能性があります。これらのデバイスは、ネットワークポート、スイッチやルーターなどのネットワークデバイスに直接接続されたり、システムコンポーネント内にワイヤレスインターフェースカードとして挿入されたりする可能性もあります。 ワイヤレスデバイスまたはネットワークが企業の知らない間にインストールされた場合、攻撃者はネットワークに容易に、かつ「認識されずに」侵入できます。このような未承認のアクセスポイントを検出し、削除することで、そのようなデバイスが攻撃に利用される期間と可能性を減らすことができます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 承認されていないワイヤレスアクセスポイントを特定し、定期的に対処する。 **適用上の注意** 攻撃者は会社のポリシーを読んで従うわけではないので、ワイヤレス技術の使用を禁止するポリシーが存在する場合でも、この要件は適用される。 この要件を満たすために使用される方法は、認可されたデバイスと認可されていないデバイス（許可されたデバイスに付随する未許可のデバイスを含む）の両方を検出および識別するのに十分でなければならない。		**グッドプラクティス** 環境内に不正なワイヤレスアクセスポイントがインストールされていないことを確実にするための適切なツールとプロセスは、環境の規模と複雑度によって決まります。 例えば、ショッピングモールの独立型キオスクでは、すべての通信コンポーネントが改ざん防止機能の付いた、または改ざんを記録するケースに収納されているため、不正なワイヤレスアクセスポイントが接続またはインストールされていないことを保証するには、詳細な物理検査を行うだけで十分な場合があります。しかし、複数のノードが存在する環境（大規模な小売店、コールセンター、サーバルーム、データセンターなど）では、詳細な物理的検査が困難な場合があります。この場合、ワイヤレスアナライザーの結果と合わせてシステムの物理的な検査を行うなど、複数の方法を組み合わせて対応することができます。 **定義** 不正アクセスポイント検出とも呼ばれます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		例 使用可能な方法は、ワイヤレスネットワークスキャン、システムコンポーネントやインフラの物理的／論理的検査、ネットワークアクセスコントロール（NAC）、またはワイヤレス IDS／IPS などですが、これらに限定されません。NAC とワイヤレス IDS／IPS は自動化された監視ツールの一例です。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.2.2 承認されているワイヤレスアクセスポイントのインベントリが、文書化されたビジネス上の正当な理由を含めて、維持される。	**11.2.2** 文書を調査して、承認されているワイヤレスアクセスポイントのインベントリが維持されていること、および、すべての承認されているワイヤレスアクセスポイントについてビジネス上の正当性が文書化されていることを確認する。	承認されているワイヤレスアクセスポイントのインベントリを作成することで、不正なワイヤレスアクセスポイントが検出された場合に、管理者が迅速に対応することができます。これにより、カード会員データ環境（CDE）が悪意のある人物にさらされるのを未然に防ぐことができます。
カスタマイズアプローチの目的		**グッドプラクティス**
承認されていないワイヤレスアクセスポイントを承認されているワイヤレスアクセスポイントと間違えない。		ワイヤレススキャナーを使用する場合、会社のネットワークに接続されていないものの、通常スキャン中に検出される既知のアクセスポイントのリストを定義しておくことも同様に重要です。これらの企業の管理外のデバイスは、マルチテナントの建物や、互いに近くにある企業でよく見られます。しかし、これらのデバイスが、企業のネットワークポートに接続されていないか、または別のネットワーク接続デバイスを介して接続されていないか、また、近隣の企業に似た SSID を与えられていないかを確認することが重要です。スキャン結果は、そのようなデバイスと、これらのデバイスが「無視できる」と判断された方法を記載する必要があります。 さらに、カード会員データ環境（CDE）に対する脅威であると判断された承認されていないワイヤレスアクセスポイントの検出は、要件 12.10.1 による事業体のインシデント対応計画に従って管理されるものとします。

要件とテスト手順		ガイダンス
11.3 外部および内部の脆弱性を定期的に特定し、優先順位をつけ、対処している。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.3.1 内部脆弱性スキャンは、以下のように実施する。 • 少なくとも 3 カ月に 1 回は実施する。 • 高リスクおよび重要な脆弱性（要件 6.3.1 で定義された事業体の脆弱性リスクランキングに基づく）が解決される。 • 再スキャンを実施し、上記の高リスクおよび重要な脆弱性がすべて解決されていることを確認する。 • スキャンツールは、常に最新の脆弱性情報に更新されている。 • スキャンは有資格者によって実施され、テスト担当者の組織的な独立性が確保されている。	**11.3.1.a** 過去 12 カ月間の内部スキャンレポート結果を調べ、直近の 12 カ月間に少なくとも 3 カ月に 1 回内部スキャンが実施されていることを確認する。	脆弱性を迅速に特定し、対処することで、脆弱性が悪用される可能性、システムコンポーネントまたはカード会員データの漏洩の可能性を低減することができます。少なくとも 3 カ月ごとに実施される脆弱性スキャンは、この検出と特定を可能にします。
	11.3.1.b 過去 12 カ月に実行した各スキャンおよび再スキャンの内部スキャンレポート結果を調べ、（PCI DSS 要件 6.3.1 で特定された）高リスクおよび重要な脆弱性がすべて解決されていることを確認する。	**グッドプラクティス**
	11.3.1.c スキャンツールの構成を調査し、担当者にインタビューして、スキャンツールが最新の脆弱性情報に更新されていることを確認する。	環境に最大のリスクをもたらす脆弱性（たとえば、要件 6.3.1 により高または重要とランク付けされたもの）は、最も高い優先度で解決する必要があります。 四半期ごとのスキャンプロセスでは、複数のスキャンレポートを組み合わせることで、3 カ月の脆弱性スキャンサイクルの一部として、すべてのシステムがスキャンされ、該当するすべての脆弱性が解決されたことを示すことができます。しかし、改善されていない脆弱性が解決されつつあることを確認するために、追加の文書が必要となる場合があります。
カスタマイズアプローチの目的	**11.3.1.d** 責任者にインタビューし、スキャンが適格な内部リソースまたは適格な外部第三者によって実行されたこと、およびテスターの組織的独立性が存在することを確認する。	
ネットワーク内部で動作する脆弱性を検出するために設計された自動化ツールを使用して、すべてのシステムコンポーネントのセキュリティ耐性を定期的に確認している。検出された脆弱性は、正式なリスク評価フレームワークに基づいて評価され、是正される。		
(次ページに続く)		*(次ページに続く)*

要件とテスト手順		ガイダンス
QSA または ASV を使用して内部脆弱性スキャンを実施する必要はない。		スキャンは少なくとも 3 カ月に 1 回必要ですが、ネットワークの複雑さ、変更の頻度、使用するデバイス、ソフトウェア、オペレーティングシステムの種類によっては、より頻繁にスキャンを行うことが推奨されます。 **定義** 脆弱性スキャンとは、外部および内部のデバイスやサーバに対して実行される自動化されたツール、技術、および／または手法の組み合わせであり、悪意のある個人が発見し悪用する可能性のあるアプリケーション、オペレーティングシステム、およびネットワークデバイスの潜在的脆弱性を明らかにするために設計されたものです。
適用上の注意 内部脆弱性スキャンは、スキャン対象のシステムコンポーネントから合理的に独立した有資格の内部スタッフ（例えば、ネットワーク管理者はネットワークのスキャンに責任を持つべきではない）が行うことができ、事業体は脆弱性スキャンを専門とする事業体に内部脆弱性スキャンを実施させることを選択することも可能です。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.3.1.1 他のすべての該当する脆弱性（要件 6.3.1 における事業体の脆弱性リスクランキングにより高リスクまたは重要としてランク付けされていないもの）は、以下のように管理される。 • 要件 12.3.1 に定めるすべての要素に従って実施される事業体のターゲットリスク分析で定義されたリスクに基づいて対処される。 • 必要に応じて再スキャンを実施する。	**11.3.1.1.a** 他のすべての該当する脆弱性（要件 6.3.1 における事業体の脆弱性リスクランキングで高リスクまたは重要としてランク付けされていないもの）に対処するためのリスクを定義する事業体のターゲットリスク分析を調べ、リスク分析が要件 12.3.1 で規定されるすべての要素に従って実施されたことを確認する。	すべての脆弱性は、重要度に関係なく、潜在的な攻撃経路となるため、定期的に対処する必要があり、最もリスクが高い脆弱性には、より迅速に対処して攻撃の可能性を制限します。
カスタマイズアプローチの目的	**11.3.1.1.b** 担当者にインタビューし、内部スキャンのレポート結果または他の文書を調査して、他のすべての該当する脆弱性（要件 6.3.1 の事業体の脆弱性リスクランキングで高リスクまたは重要として位置付けられていないもの）が、事業体のターゲットリスク分析で定義したリスクに基づいて対処され、スキャンプロセスには脆弱性に対処したことを確認するため必要に応じて再スキャンが含まれることを確認する。	
ランクが低い脆弱性（高または重要より低い）には、事業体のリスクに応じた頻度で対処している。		
適用上の注意		
低リスクの脆弱性に対処する時間枠は、要件 12.3.1 によるリスク分析の結果に従う。この分析には、（最低限）保護対象の資産、脅威、および脅威が実現する可能性または影響度の特定が含まれる。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 認証スキャンは、非認証スキャンでは検出できない脆弱性を検出できるため、事業体の脆弱性ランドスケープをより深く理解することができます。いくつかの脆弱性は認証スキャンのみで検出されるため、攻撃者は事業体が気づいていない脆弱性を利用する可能性があります。 認証スキャンは、組織の脆弱性に関する重要な追加情報を提供することができます。 **グッドプラクティス** これらのスキャンに使用される認証情報は、高度に特権的とみなされるべきです。これらは、PCI DSS 要件 7 および 8 に従って保護および制御する必要があります（ただし、多要素認証 やアプリケーションおよびシステムアカウントに関する要件は除きます）。
11.3.1.2 内部脆弱性スキャンは、以下のように認証スキャンで実施します。 • 認証スキャンのための認証情報を受け入れることができないシステムは、文書化される。 • スキャンのために認証情報を受け入れるシステムには、十分な権限が使用されています。 • 認証スキャンに使用したアカウントが対話的ログインに使用できる場合は、要件 8.2.2 に従って管理される。	**11.3.1.2.a** スキャンツールの設定を調査し、スキャンのために認証情報を受け入れるシステムにおいて、認証スキャンが十分な特権で内部スキャンに使用されていることを確認する。	
	11.3.1.2.b スキャンレポート結果を調査し、担当者にインタビューして、認証スキャンが実行されていることを確認する。	
	11.3.1.2.c 認証スキャンに使用されたアカウントが対話的ログインに使用できる場合、アカウントを調査し、担当者にインタビューして、要件 8.2.2 で指定されたすべての要素に従ってアカウントが管理されていることを確認する。	
カスタマイズアプローチの目的	**11.3.1.2.d** 文書を調査し、認証されたスキャンのための認証情報を受け入れることができないシステムが定義されていることを確認する。	
脆弱性の検出に使用される自動化ツールは、リモートからは見えない、各システムにローカルな脆弱性を検出することができる。		

要件とテスト手順		ガイダンス
適用上の注意 認証されたスキャンツールは、ホストベースまたはネットワークベースのいずれかを使用することができる。 「十分な」特権とは、既知の脆弱性を検出する完全なスキャンを実施できるように、システムリソースにアクセスするために必要な特権のことである。 この要件は、スキャンのために認証情報を受け入れることができないシステムコンポーネントには適用されない。スキャンのために認証情報を受け付けないシステムの例としては、一部のネットワークおよびセキュリティアプライアンス、メインフレーム、コンテナなどがある。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
11.3.1.3 大幅な変更の後には、以下のように内部スキャンが実施される。 • 高リスクおよび重要な脆弱性（要件 6.3.1 で定義された事業体の脆弱性リスクランキングに基づく）が解決される。 • 必要に応じて再スキャンを実施する。 • スキャンは有資格者によって実施され、テスターの組織的独立性が確保されている（QSA または ASV である必要はない）。	**11.3.1.3.a** 変更管理文書および内部スキャン報告書を調査し、大幅な変更後にシステムコンポーネントがスキャンされたことを確認する。	**目的** 大幅な変更後に環境をスキャンすることで、変更が適切に完了し、その変更によって環境のセキュリティが損なわれないことを確認します。 **グッドプラクティス** 事業体は、要件 6.5.2 による変更プロセスの一環として、また変更が完了したとみなす前に、大幅な変更後のスキャンを実行する必要があります。変更の影響を受けるすべてのシステムコンポーネントをスキャンする必要があります。
	11.3.1.3.b 担当者にインタビューを行い、内部スキャンおよび再スキャンレポートを調査し、大幅な変更後に内部スキャンが実行され、要件 6.3.1 に定義されている高リスクおよび重要な脆弱性が解決されていることを確認する。	
カスタマイズアプローチの目的 ネットワークまたはシステムに大幅な変更が加えられた場合、ネットワーク内部で動作する脆弱性を検出するために設計された自動化ツールを使用して、すべてのシステムコンポーネントのセキュリティ状態を検証することができる。検出された脆弱性は、正式なリスク評価フレームワークに基づいて評価され、是正される。	**11.3.1.3.c** 担当者にインタビューし、内部スキャンが有資格の内部リソースまたは有資格の外部第三者によって実施されていること、およびテスターの組織的独立性が存在することを確認する。	
適用上の注意 要件 11.3.1.2 による認証された内部脆弱性スキャンは、大幅な変更後に実施されるスキャンには必要ない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.3.2 外部からの脆弱性スキャンは、以下のように実施される。 • 少なくとも 3 カ月に 1 回は実施する。 • PCI SSC 認定スキャンニングベンダ(ASV)によって実施する。 • 脆弱性が解決され、ASV プログラムガイドの合格スキャンの要件が満たされている。 • 必要に応じて再スキャンを行い、合格スキャンのための ASV プログラムガイドの要件に従って脆弱性が解決されることを確認する。	**11.3.2.a** 過去 12 カ月間の ASV スキャンレポートを調査し、直近の 12 カ月間に外部脆弱性スキャンが 3 カ月に 1 回以上実施されていることを確認する。	攻撃者は日常的に、パッチが適用されていない、または脆弱な外部向けサーバを探しており、それらを利用して直接攻撃を仕掛けることができます。組織は、これらの外部向けデバイスの脆弱性を定期的にスキャンし、脆弱性にパッチを適用するか修復して、事業体を保護する必要があります。 外部ネットワークは侵害のリスクが高いため、外部脆弱性スキャンは PCI SSC 認定スキャニングベンダ（ASV）により少なくとも 3 か月に 1 回実行する必要があります。
カスタマイズアプローチの目的	**11.3.2.b** 過去 12 カ月に実施した各スキャンおよび再スキャンの ASV スキャンレポート結果を調査し、脆弱性が解決され、ASV プログラムガイドの合格のための要件が満たされていることを確認する。	**グッドプラクティス** スキャンは少なくとも 3 カ月に 1 回必要ですが、ネットワークの複雑さ、変更の頻度、使用するデバイス、ソフトウェア、オペレーティングシステムの種類によっては、より頻繁にスキャンを行うことが推奨されます。 複数のスキャンレポートを組み合わせることで、すべてのシステムがスキャンされ、3 カ月の脆弱性スキャンサイクルの一部として該当するすべての脆弱性が解決されたことを示すことができます。ただし、改善されていない脆弱性が解決されつつあることを確認するために、追加の文書が必要な場合があります。
この要件は、カスタマイズアプローチの対象外である。	**11.3.2.c** ASV スキャンレポートを調査し、スキャンが PCI SSC 認定スキャンニングベンダ（ASV）によって完了したことを確認する。	

要件とテスト手順		ガイダンス
適用上の注意 PCI DSS 初回準拠の場合、以下の点を評価者が確認すれば、12 か月以内に 4 回の合格スキャンを完了する必要はない。1) 直近のスキャン結果が合格であること、2) 事業体が少なくとも 3 カ月に 1 回のスキャンを義務付ける方針と手順を文書化していること、3) スキャン結果に示された脆弱性が再スキャンで修正されていることを評価者が確認していること。 ただし、初回の PCI DSS 審査以降の年については、少なくとも 3 カ月に一度スキャンに合格していることが必要である。 ASV スキャンツールは、膨大な数のネットワークタイプおよびトポロジーをスキャンすることができる。対象環境に関する詳細（ロードバランサ、サードパーティプロバイダ、ISP、特定の構成、使用中のプロトコル、スキャンの干渉など）については、ASV とスキャンの顧客との間で調整する必要がある。 スキャン顧客の責任、スキャンの準備などについては、PCI SSC のウェブサイトで公開されている *ASV プログラムガイド*を参照すること。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.3.2.1 外部スキャンは、大幅な変更後に以下のように実施する。 • CVSS スコアで 4.0 以上の脆弱性が解決されていること。 • 必要に応じて再スキャンを実施する。 • スキャンは有資格者によって実施され、テスターの組織的独立性が確保されている（QSA または ASV である必要はない）。	**11.3.2.1.a** 変更管理文書および外部スキャンレポートを調査し、大幅な変更後にシステムコンポーネントがスキャンされたことを確認する。	大幅な変更後に環境をスキャンすることで、変更が適切に完了し、その変更によって環境のセキュリティが損なわれないことを確認します。
	11.3.2.1.b 担当者にインタビューし、外部スキャンおよび再スキャンレポートを調査して、大幅変更後に外部スキャンが実行され、CVSS で 4.0 以上のスコアを持つ脆弱性が解決されたことを確認する。	**グッドプラクティス** 事業体は、変更プロセスの一部として、大幅な変更後に、その変更が完了したとみなされる前にスキャンを実行する必要性を含めるべきです。変更の影響を受けるすべてのシステムコンポーネントをスキャンする必要があります。
カスタマイズアプローチの目的	**11.3.2.1.c** 担当者にインタビューし、外部スキャンが有資格の内部リソースまたは有資格の外部第三者によって実施されていること、およびテスターの組織的独立性が存在することを確認する。	
ネットワークまたはシステムに大幅な変更が加えられた場合、ネットワーク外部から操作される脆弱性を検出するために設計されたツールを使用して、すべてのシステムコンポーネントのセキュリティ状態が検証される。検出された脆弱性は、正式なリスク評価フレームワークに基づいて評価され、是正される。		

要件とテスト手順		ガイダンス
11.4 外部および内部へのペネトレーションテストを定期的に実施し、悪用可能な脆弱性およびセキュリティ上の弱点を是正している。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 攻撃者は、カード会員データにアクセスし、そのデータを流出させるために利用する外部および内部の脆弱性を見つけるために多くの時間を費やします。そのため、事業体は、攻撃者が行うのと同じように、ネットワークを徹底的にテストする必要があります。このテストにより、事業体は、事業体のネットワークとデータを侵害するために利用される可能性のある弱点を特定および修正し、そのような攻撃からネットワークとシステムコンポーネントを保護するために適切な措置を講じることができます。 **グッドプラクティス** ペネトレーションテストの技術は、組織のニーズと構造に基づいて異なり、テストされた環境に適したものでなければなりません。例えば、ファジングテスト、インジェクションテスト、フォージェリーテストが適切な場合があります。テストの種類、深さ、複雑さは、特定の環境と組織のニーズに依存します。 *(次ページに続く)*
11.4.1 侵入テストの方法論は、事業体によって定義、文書化、実施され、以下を含む。 • 業界で受け入れられているペネトレーションテストのアプローチ • カード会員データ環境（CDE）の境界全体および重要なシステムを対象としていること • ネットワークの内側と外側の両方からのテスト • セグメンテーションと適用範囲縮小制御の有効性テスト • 要件 6.2.4 に記載された脆弱性を最低限特定するためのアプリケーション層ペネトレーションテスト • オペレーティングシステムだけでなく、ネットワーク機能をサポートするすべてのコンポーネントを包含するネットワーク層のペネトレーションテスト • 過去 12 か月に経験した脅威と脆弱性のレビューと考察 *(次ページに続く)*	**11.4.1** 文書を調査し、担当者にインタビューして、事業体によって定義、文書化、実施されたペネトレーションテスト方法がこの要件で指定されたすべての要素を含むことを確認する。	

要件とテスト手順		ガイダンス
• 侵入テスト中に発見された悪用可能な脆弱性およびセキュリティ上の弱点によってもたらされるリスクを評価し、対処するための文書化されたアプローチ • 侵入テストの結果および是正活動の結果を少なくとも 12 カ月間保存していること **カスタマイズアプローチの目的** 有能な手動攻撃者による模擬的な攻撃手法により、脆弱性およびセキュリティ上の弱点を突くことを試みる徹底的な技術テストのための正式な方法論が定義されていること。 **適用上の注意** ネットワーク内部からのテスト（または「内部侵入テスト」）とは、カード会員データ環境（CDE）内部からのテストと、信頼できる内部ネットワークおよび信頼できない内部ネットワークからカード会員データ環境（CDE）に侵入するテストの両方を意味する。 *(次ページに続く)*		**定義** 侵入テストは、実際の攻撃状況をシミュレートするもので、テスト者に提供される情報の量が異なる場合、攻撃者がどこまで環境に侵入できるかを特定するものです。これにより、事業体は潜在的な露出度をよりよく理解し、攻撃から身を守るための戦略を立てることができます。侵入テストは、脆弱性スキャンとは異なります。なぜなら、侵入テストは通常、特定された脆弱性を悪用することを含む能動的なプロセスであるためです。 脆弱性のスキャンだけでは侵入テストとは言えません。また、脆弱性のスキャンで見つかった脆弱性を利用しようとすることだけに焦点を当てた場合、侵入テストは適切とは言えません。脆弱性スキャンの実施は、最初のステップの 1 つかもしれませんが、侵入テスト実施者がテスト戦略を計画するために行う唯一のステップではありません。脆弱性スキャンで既知の脆弱性が検出されなかったとしても、侵入テスト実施者は、可能性のあるセキュリティ ギャップを特定するために、システムに関する十分な知識を得ることがよくあります。 侵入テストは、非常に手作業が多いプロセスです。自動化されたツールを使用することもありますが、テスト者はシステムに関する知識を駆使し *(次ページに続く)*

要件とテスト手順		ガイダンス
ネットワーク外部からのテスト（または「外部侵入テスト」）とは、信頼されたネットワークの露出した外部境界、および公共ネットワークインフラに接続またはアクセス可能な重要なシステムをテストすることを意味する。		て、環境にアクセスすることができます。多くの場合、テスト者は、防御の層を突破することを目的として、いくつかのタイプのエクスプロイトを連鎖的に行います。例えば、テスト者がアプリケーションサーバにアクセスする方法を見つけた場合、テスト者は、侵害されたサーバをポイントとして、そのサーバがアクセスできるリソースを基に新たな攻撃を仕掛けます。このように、テスト者は、攻撃者が使用するテクニックをシミュレートすることで、環境における潜在的な弱点の領域を特定することができます。また、セキュリティ監視・検知方法のテスト（例えば、ログ記録やファイル整合性監視機構の有効性を確認する）も検討する必要があります。 **その他の情報** *情報補足*を参照してください：その他のガイダンスとして、*侵入テストのガイダンス*があります。 業界で認められている侵入テストのアプローチには、以下のものがあります： *オープンソースセキュリティテスト方法およびマニュアル（OSSTMM）。* *オープンウェブアプリケーションセキュリティプロジェクト (OWASP) の侵入テストプログラム。*

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
11.4.2 内部ペネトレーションテストを実施する。 • 事業者が定義した方法論に従っている。 • 少なくとも 12 カ月に 1 回 • インフラストラクチャまたはアプリケーションの大幅なアップグレードまたは変更後 • 認定された内部リソースまたは認定された外部第三者によるものであること • テスターの組織的な独立性がある（QSA または ASV である必要はない）。	**11.4.2.a** 直近の内部ペネトレーションテストの作業範囲と結果を調査し、ペネトレーションテストがこの要件で指定されたすべての要素に従って実施されていることを確認する。	**目的** 内部ペネトレーションテストには 2 つの目的があります。まず、外部ペネトレーションテストと同様に、内部ネットワークにある程度アクセスできた攻撃者（その攻撃者が不正な活動を行う正規ユーザであるか、事業体の境界線に侵入した外部攻撃者であるかにかかわらず）が使用し得る脆弱性や設定ミスを発見することです。 第二に、内部ペネトレーションテストは、以前は知られていなかったシステムを検出することによって、変更管理プロセスの失敗を発見するのにも役立ちます。さらに、カード会員データ環境（CDE）内で動作している多くの制御の状態を確認することができます。 ペネトレーションテストの結果は、「合格」や「不合格」に分類できるものではないため、ペネトレーションテストは本当の意味での "テスト " ではありません。 テストの最良の結果は、事業体が知らなかった脆弱性と設定ミスのカタログであり、ペネトレーション・テスターが、攻撃者より先にそれらを発見することです。何も発見できなかったペネトレーションテストは、通常、事業体のセキュリティ体制を正しく反映したものではなく、ペネトレーション・テスターの欠点を示しています。
カスタマイズアプローチの目的 内部システムの防御は、進化する新しい攻撃や脅威に対処し、大幅な変更が未知の脆弱性を導入しないことを保証するために必要な頻度で、事業体が定義した方法論に従って、技術的テストにより検証されます。	**11.4.2.b** 担当者にインタビューし、内部ペネトレーションテストが認定された内部リソースまたは認定された外部第三者によって実施されたこと、およびテスターの組織的独立性が存在することを確認する（QSA または ASV である必要はない）。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**グッドプラクティス** ペネトレーションテストを実施する資格のあるリソースを選択する際に考慮すべき点は以下の通りです。 • 特定のペネトレーションテストの認定資格は、テスターのスキルレベルおよび能力の指標となる可能性があります。 • ペネトレーションテストの実施経験、例えば、経験年数、過去の業務の種類と範囲などは、テスト実施者の経験が業務の必要性に適しているかどうかを確認するのに役立つ場合があります。 **その他の情報** 追加のガイダンスとして、PCI SSC ウェブサイトの *情報補足：ペネトレーションテストのガイダンス* を参照してください。
11.4.3 外部ペネトレーションテストを実施する。 • 事業体が定義した方法論に従う • 少なくとも 12 カ月に 1 回 • インフラストラクチャまたはアプリケーションの大幅なアップグレードまたは変更後 • 認定された内部リソースまたは認定された第三者によるものである • テスターの組織的な独立性がある（QSA または ASV である必要はない）。	**11.4.3.a** 直近の外部ペネトレーションテストの作業範囲と結果を調査し、ペネトレーションテストがこの要件に規定されるすべての要素に従って実施されていることを確認する。 **11.4.3.b** 担当者にインタビューし、外部ペネトレーションテストが認定された内部リソースまたは認定された第三者によって実施されたこと、およびテスターの組織的独立性が存在することを確認する（QSA または ASV である必要はない）。	
カスタマイズアプローチの目的 外部システムの防御は、進化する新しい攻撃や脅威に対処し、大幅な変更が未知の脆弱性をもたらさないようにするために、必要に応じて頻繁に、事業体の定義した手法に従ってテクニカルテストにより検証される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
11.4.4 ペネトレーションテストで発見された悪用可能な脆弱性およびセキュリティ上の弱点は、以下のように修正される。 • 要件 6.3.1 に定義されている、セキュリティ上の問題によってもたらされるリスクに関する事業体の評価に従って。 • 修正内容を確認するために、ペネトレーションテストが繰り返される。	**11.4.4** ペネトレーションテストの結果を調べ、指摘された悪用可能な脆弱性およびセキュリティ上の弱点が、この要件に規定されたすべての要素に従って修正されたことを確認する。	**目的** ペネトレーションテストの結果は、通常、演習によって発見された脆弱性の優先順位付けされたリストです。多くの場合、テスターは、システムコンポーネントを侵害するために、いくつかの脆弱性を連鎖させることになります。ペネトレーションテストで発見された脆弱性を修正することで、同じ脆弱性が悪意のある攻撃者によって悪用される確率を大幅に減らすことができます。 事業体独自の脆弱性リスク評価プロセス（要件 6.3.1 を参照）を使用することで、事業体に最も高いリスクをもたらす脆弱性をより迅速に是正することができます。 **グッドプラクティス** 事業体のリスク評価の一環として、事業体は、脆弱性が悪用される可能性がどの程度あるか、また、リスクを低減するための他の管理策が環境内に存在するかどうかを検討する必要があります。 PCI DSS 要件が満たされていないことを指摘するような弱点があれば、対処する必要があります。
カスタマイズアプローチの目的		
システム防御の検証中に発見された脆弱性およびセキュリティ上の弱点が緩和されていることである。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
11.4.5 カード会員データ環境（CDE） を他のネットワークから分離するためにセグメンテーションが使用されている場合、セグメンテーション制御に対してペネトレーションテストを以下のように実施する。 • 少なくとも 12 カ月に一度、およびセグメンテーション制御／方法に変更があった後 • 使用しているすべてのセグメンテーション制御／方法を対象としていること。 • 事業体が定義したペネトレーションテストの方法論に従っていること。 • セグメンテーション制御／方法が運用されており、効果的であること、およびカード会員データ環境（CDE）が適用範囲外のすべてのシステムから分離されていることを確認すること。 • セキュリティレベルの異なるシステムを分離するために隔離を使用した場合の有効性を確認する（要件 2.2.3 を参照）。 • 認定された内部リソースまたは認定された第三者によって実施される。 • テスターの組織的な独立性がある（QSA または ASV である必要はない）。 *(次ページに続く)*	**11.4.5.a** セグメンテーション制御を調べ、ペネトレーションテスト方法をレビューして、この要件で指定されたすべての要素に従って、すべてのセグメンテーション方法をテストするためにペネトレーションテスト手順が定義されていることを確認する。 **11.4.5.b** 最新のペネトレーションテストの結果を調べ、ペネトレーションテストがこの要件で指定されたすべての要素をカバーし、対処していることを確認する。 **11.4.5.c** 担当者にインタビューを行い、テストが認定された内部リソースまたは認定された第三者によって実施されたこと、およびテスターの組織的独立性が存在することを確認する（QSA または ASV である必要はない）。	**目的** カード会員データ環境 (CDE)を信頼できない内部ネットワークから隔離するためにセグメンテーション制御を使用する場合、カード会員データ環境（CDE）のセキュリティはそのセグメンテーションが機能することに依存します。多くの攻撃は、攻撃者が隔離されたネットワークから カード会員データ環境（CDE）内へ横方向に移動することを含んでいます。信頼できないネットワークが本当にカード会員データ環境（CDE）から分離されているかどうかを検証するために、ペネトレーションテストのツールと技術を使用することで、セグメンテーション制御の失敗または誤設定について事業体に警告し、それを是正することができます。 **グッドプラクティス** ホスト発見やポートスキャンなどの技術は、適用範囲外のセグメントがカード会員データ環境（CDE）にアクセスできないことを確認するために使用することができます。

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 セグメンテーションが使用されている場合、技術テストにより、カード会員データ環境（CDE）をすべての適用範囲外システムから分離する上で、変更後を含め継続的に有効であることが定期的に検証される。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.4.6 ***サービスプロバイダのみに対する追加要件：*** カード会員データ環境（CDE） を他のネットワークから分離するためにセグメンテーションが使用されている場合、セグメンテーション制御について以下のようにペネトレーションテストが実施される。	**11.4.6.a** ***サービスプロバイダ評価のみの追加テスト手順：***最新のペネトレーションテストの結果を調べ、ペネトレーションテストがこの要件で指定されたすべての要素をカバーし、対処していることを確認する。	サービスプロバイダは通常、より大量のカード会員データにアクセスでき、また、他の複数の事業体を侵害するために悪用される可能性のある入口ポイントを提供することができます。 *(次ページに続く)*

要件とテスト手順		ガイダンス
• 少なくとも半年に一度、セグメンテーション制御／方法を変更した後。 • 使用しているすべてのセグメンテーション制御／方法を対象としていること。 • 事業体が定義したペネトレーションテストの方法論に従っていること。 • セグメンテーション制御／方法が運用されており、効果的であること、およびカード会員データ環境（CDE）が適用範囲外のすべてのシステムから分離されていることを確認すること。 • セキュリティレベルの異なるシステムを分離するためにセグメンテーションを使用した場合の有効性を確認する（要件 2.2.3 を参照）。 • 認定された内部リソースまたは認定されたサードパーティによって実施される。 • テスターの組織的な独立性がある（QSA または ASV である必要はない）。 *(次ページに続く)*	**11.4.6.b *サービスプロバイダ評価のみの追加テスト手順：***担当者にインタビューし、テストが認定された内部リソースまたは認定された第三者によって実施されたこと、 およびテスターの組織的独立性が存在することを確認する（QSA または ASV である必要はない）。	また、サービスプロバイダは通常、より大規模で複雑なネットワークを持っており、より頻繁に変更される可能性があります。サービスプロバイダ環境では、複雑で動的なネットワークでセグメンテーション制御が失敗する確率がより高くなります。 セグメンテーション制御の検証をより頻繁に行うことで、攻撃者が適用範囲外の信頼できないネットワークから カード会員データ環境（CDE）に横方向にピボットしようとする前に、そのような障害を発見できる可能性があります。 **グッドプラクティス** 要件では、この範囲の検証は 6 カ月ごとおよび大幅な変更の後に実施されると指定されていますが、カード会員データ環境（CDE）を他のネットワークから分離する効果を維持するために、この演習はできるだけ頻繁に実行されるべきです。
カスタマイズアプローチの目的 セグメンテーションを使用する場合、技術テストにより、カード会員データ環境（CDE）を適用範囲外のシステムから分離する上で、変更後を含め継続的に有効であることが確認される。		

要件とテスト手順		ガイダンス
適用上の注意 この要件は、評価対象組織がサービスプロバイダである場合にのみ適用される。		
定義されたアプローチの要件 **11.4.7** ***マルチテナントサービスプロバイダーのみの追加要件:*** *マルチテナント型サービス事業者は、要件 11.4.3 及び 11.4.4 に従い、外部侵入試験について顧客をサポートする。*	**定義されたアプローチのテスト手順** **11.4.7** ***マルチテナント型サービス事業者のみの追加試験手順:*** *マルチテナント型サービスプロバイダが、要件 11.4.3 および 11.4.4 に従った外部侵入テストを顧客にサポートしていることを確認するための証拠を調査する。*	**目的** 事業者は、PCI DSS に準拠した侵入テストを実施し、攻撃者の行動をシミュレートして、自社環境の脆弱性を発見する必要があります。共有環境およびクラウド環境では、マルチテナント型サービスプロバイダは、侵入テスト実施者の活動が他の顧客のシステムに影響することを懸念する場合があります。 マルチテナントのサービスプロバイダは、顧客のシステムが悪用される可能性があるため、侵入テストを禁止することはできません。そのため、マルチテナント型サービス事業者は、顧客からの侵入テストの実施要請や侵入テストの結果をサポートしなければならない。
カスタマイズアプローチの目的 マルチテナントのサービスプロバイダは、技術的テストへのアクセスを提供するか、同等の技術的テストが実施されたことを証明することによって、顧客の技術的テストの必要性をサポートします。 *(次ページに続く)*		

要件とテスト手順		ガイダンス
適用上の注意 この要件は、評価対象企業がマルチテナント型サービス事業者である場合にのみ適用されます。 この要件を満たすために、マルチテナントサービスプロバイダーは、以下のいずれかを行うことができる。 • 顧客の契約インフラに対して要件 11.4.3 および 11.4.4 に従ってペネトレーションテストが実施されたことを示す証拠を顧客に提供する、または • 顧客自身がペネトレーションテストを実施できるように、各顧客に迅速なアクセスを提供する。 顧客に提供する証拠には、編集したペネトレーションテストの結果を含めることができるが、要件 11.4.3 および 11.4.4 のすべての要素が顧客のために満たされていることを証明する十分な情報を含める必要がある。 も参照してください A1 マルチテナント型サービスプロバイダに対する追加の PCI DSS 要件 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
11.5 ネットワークへの侵入および予期しないファイルの変更が検出され、対応される。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
11.5.1 ネットワークへの侵入を検知および／または防止するために、以下のような侵入検知技術および／または侵入防止技術が使用されている。 • カード会員データ環境（CDE）の境界において、すべてのトラフィックを監視する。 • カード会員データ環境（CDE）内の重要なポイントにおいて、すべてのトラフィックを監視する。 • 担当者は侵入の疑いがあることを警告される。 • すべての侵入検知・防止エンジン、ベースライン、およびシグネチャが最新に保たれている。	**11.5.1.a** システム構成とネットワーク図を調べ、すべてのトラフィックを監視するために、侵入検知および／または侵入防止技術が導入されていることを確認する。 • カード会員データ環境（CDE） の境界において。 • カード会員データ環境（CDE）内の重要なポイントにおいて。	**目的** 侵入検知および／または侵入防止技術（IDS/IPS など）は、ネットワークに入ってくるトラフィックを、何千もの侵害タイプ（ハッカーツール、トロイの木馬、その他のマルウェア）の既知の「シグネチャ」または挙動と比較し、試みが発生した時点で警告を送ったり、停止させたりするものです。不正な活動を検知するためのプロアクティブなアプローチがなければ、コンピュータリソースへの攻撃（または不正使用）に長期間気付かれない可能性があります。カード会員データ環境（CDE）への侵入がもたらす影響は、多くの場合、攻撃者が検知されるまでに環境内に留まる時間によるものです。
	11.5.1.b システム構成を調査し、責任者にインタビューして、侵入検知および／または侵入防止技術が、侵害の疑い があることを担当者に警告していることを確認する。	**グッドプラクティス** これらの技術によって発生するセキュリティ警告を継続的に監視し、侵入の試みまたは実際の侵入を阻止し、潜在的な損害を抑えることができるようにする必要があります。
カスタマイズアプローチの目的	**11.5.1.c** システム構成およびベンダの文書を調査し、侵入検知および／または侵入防止技術が、すべてのエンジン、ベースラインおよびシグネチャを最新の状態に維持するように構成されていることを確認する。	**定義** 重要な場所には、ネットワークセグメント間（例えば、DMZ と内部ネットワーク間、または適用範囲内と適用範囲外のネットワーク間） *(次ページに続く)*
脅威者の活動を示唆する疑わしい、または異常なネットワークトラフィックをリアルタイムで検出するメカニズムが実装されている。これらのメカニズムによって生成されたアラートは、検知された活動の結果としてシステムコンポーネントが侵害されないことを保証するために、担当者または自動化された手段によって対応される。		

要件とテスト手順		ガイダンス
		のネットワークセキュリティコントロールや、信頼性の低いシステムコンポーネントと信頼性の高いシステムコンポーネント間の接続を保護するポイントが含まれますが、これらに限定されるものではありません。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.5.1.1 ***サービスプロバイダのみに対する追加要件：***侵入検知および／または侵入防止技術が、マルウェアの秘密の通信経路を検知し、警告し／防止し、対処する。	**11.5.1.1.a** ***サービスプロバイダ評価のみの追加テスト手順：***文書と構成設定を調査し、秘密のマルウェア通信チャネルを検出し、警告し、防止する方法が設置され、運用されていることを確認する。	マルウェアの秘密通信（DNS トンネリングなど）を検知することで、ネットワーク内部でのマルウェアの横展開やデータの流出を阻止することができます。この制御を行う場所を決定する際、事業体はネットワーク内の重要な場所と、秘密の通信路の可能性が高い経路を考慮する必要があります。 マルウェアが感染した環境に足場を築く場合、多くの場合、コマンド＆コントロール（C&C）サーバへの通信経路を確立しようとします。 *(次ページに続く)*
	11.5.1.1.b ***サービスプロバイダ評価のみの追加テスト手順：***事業体のインシデントレスポンス計画（要件 12.10.1）を調査し、秘密のマルウェア通信チャネルが検出された場合の対応を要求し定義していることを確認する。	

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 コマンド＆コントロールシステムとの秘密通信を検知し、警告・防止するメカニズムが存在する。これらのメカニズムによって発生した警告には、担当者、またはそのような通信がブロックされることを確認する自動化された手段が対応する。 **適用上の注意** この要件は、評価対象組織がサービスプロバイダである場合にのみ適用される。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*	**11.5.1.1.c** ***サービスプロバイダ評価のみの追加テスト手順：***責任者にインタビューを行い、プロセスを観察することで、担当者がマルウェアの通信・制御技術に関する知識を維持し、マルウェアが疑われる場合の対応方法について知識を有していることを確認する。	攻撃者は、C&C サーバを通じて、 感染したシステム上のマルウェアと通信し、 これを制御して、悪意のあるペイロードや指示を配信したり、データの流出を開始したりします。多くの場合、マルウェアはボットネットを介して間接的に C&C サーバと通信し、監視を迂回し、コントロールをブロックし、秘密のチャネルを検出できない様にこれらの方法を無効化します。 **グッドプラクティス** マルウェアの通信経路を検知して対処する方法としては、リアルタイムエンドポイントスキャン、発信トラフィックのフィルタリング、「許可」リスト、データ損失防止ツール、IDS/IPS などのネットワークセキュリティ監視ツールなどがあります。さらに、DNS のクエリおよびレスポンスは、インシデントレスポンスや侵入の発見をサポートするために、ネットワーク防御者が使用する重要なデータソースとなっています。これらのトランザクションが処理および分析のために収集されると、多くの貴重なセキュリティ分析シナリオが可能になります。 マルウェアの動作モードに関する最新の知識を維持することは重要であり、これを緩和することは、環境におけるマルウェアの影響を検出し制限するのに役立つからです。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
11.5.2 変更検出メカニズム（例えば、ファイル整合性監視ツール）は、以下のように展開される。 • 重要なファイルの不正な変更（変更、追加、削除を含む）を担当者に警告すること。 • 少なくとも週 1 回、重要ファイルの比較を行うこと。	**11.5.2.a** システム設定、監視対象ファイル、監視活動の結果を調査し、変更検出メカニズムの使用を確認する。 **11.5.2.b** 変更検出メカニズムの設定を調査し、この要件で指定されたすべての要素に従って構成されていることを確認する。	重要なシステムファイル、設定ファイル、コンテンツファイルの変更は、攻撃者が組織のシステムにアクセスしたことを示す指標となり得ます。このような変更は、攻撃者が検知または記録されることなく、さらなる悪意ある行為、カード会員データへのアクセス、および／または活動を行うことを可能にする可能性があります。 変更検出メカニズムは、重要なファイルへのこのような変更を検出して評価し、アラートを生成し、定義されたプロセスに従って対応できるようにすることで、担当者が適切な行動を取れるようにします。 適切に実装されず、変更検出ソリューションの出力が監視されていない場合、悪意のある個人が設定ファイルのコンテンツ、オペレーティングシステムプログラム、またはアプリケーション実行ファイルを追加、削除、または変更する可能性があります。不正な変更が検出されないと、既存のセキュリティコントロールが無効になり、通常の処理に影響を与えることなく、カード会員データが盗まれる可能性があります。 *(次ページに続く)*
カスタマイズアプローチの目的		
重要なファイルは、警告が生成されることなく、権限のない者によって変更されることがない。		
適用上の注意		
変更検出の目的では、重要なファイルとは通常、定期的に変更されないが、その変更がシステム危殆化または危殆化のリスクを示す可能性があるものをいう。ファイル整合性監視製品などの変更検出メカニズムには、通常、関連するオペレーティングシステムの重要なファイルがあらかじめ設定されています。その他の重要なファイル、例えばカスタムアプリケーションのためのファイルは、事業体（つまり、加盟店またはサービスプロバイダ）によって評価され、定義されなければならない。		

要件とテスト手順		ガイダンス
		グッドプラクティス 監視すべきファイルの例としては、以下のものが挙げられるが、これらに限定されません。 • システム実行ファイル • アプリケーションの実行ファイル • 設定ファイルおよびパラメータファイル • 一元保存、履歴、またはアーカイブされた監査ログ。 • 事業体によって決定されたその他の重要なファイル（例えば、リスクアセスメントまたはその他の手段を通じて）。 **例** ファイル整合性監視（FIM）ツールなどの変更検出ソリューションは、重要なファイルの変更、追加、削除をチェックし、そのような変更が検出されたときに通知します。

要件とテスト手順		ガイダンス
11.6 決済ページの不正な変更が検知され、対応されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
11.6.1 変更・改ざん検知のメカニズムは、以下のように展開されている。 • 消費者ブラウザが受信した HTTP ヘッダーと決済ページのコンテンツに対する不正な変更 (侵害の指標、変更、追加、および削除を含む) を担当者に警告すること。 • メカニズムは、受信した HTTP ヘッダーと決済ページを評価するように構成される。 • メカニズムの機能は、以下のように実行される。 – 少なくとも 7 日に 1 回 **または** – 定期的に（要件 12.3.1 に規定されたすべての要素に従って実施される事業体のターゲットリスク分析で定義された頻度で）	**11.6.1.a** システム設定、監視された決済ページ、および監視活動の結果を調査し、変更および改ざん検知メカニズムが使用されていることを確認する。 **11.6.1.b** 構成設定を調べて、この要件で指定されたすべての要素に従ってメカニズムが構成されていることを確認する。 **11.6.1.c** メカニズム機能が事業体定義の頻度で実行される場合、頻度を決定するための事業体のターゲットリスク分析を調べ、リスク分析が要件 12.3.1 に規定するすべての要素に従って実行されたことを確認する。 **11.6.1.d** コンフィギュレーション設定を調べ'担当者にインタビューを行い、メカニズムの機能では次のどちらかが実行されているかを確認する。 • 少なくとも 7 日に 1 回 **または** • この要件のために実施された事業体のターゲットリスク分析で定義された頻度で。	**目的** 多くのウェブページは、現在、アクティブコンテンツ（主に JavaScript）を含むオブジェクトを、インターネットの複数の場所から組み立てることに依存しています。さらに、多くのウェブページのコンテンツは、コンテンツ管理システムやタグ管理システムを使って定義されており、従来の変更検出メカニズムでは監視できない場合があります。 したがって、悪意のある活動による変更や指標を検出する唯一の場所は、ページが構築され、すべての JavaScript が解釈される消費者ブラウザの中です。 消費者ブラウザが受信した HTTP ヘッダーの最新バージョンと決済ページのアクティブコンテンツを、以前のバージョンまたは既知のバージョンと比較することにより、スキミング攻撃を示唆する不正な変更を検出することが可能です。 さらに、既知の侵害の指標や、スキマーに典型的なスクリプト要素や動作を探すことで、疑わしいアラートを発することができます。 *(次ページに続く)*
カスタマイズアプローチの目的		
電子商取引のスキミングコードやテクニックは、消費者ブラウザが受信した決済ページに、適時警告を発生させることなく追加することはできません。迅速な警告が生成されない限り、スキミング防止策を決済ページから削除することはできない。		

要件とテスト手順		ガイダンス
適用上の注意 この要求の意図は、事業者が消費者のシステムやブラウザにソフトウェアをインストールすることではなく、事業者がガイダンス欄の「例」に記載されているような技術を使用して、予期しないスクリプト活動を防止・検出することである。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		**例** 決済ページのヘッダーやコンテンツの変更を検知して報告するメカニズムには、以下のようなものがありますが、これらに限定されるものではありません。 • コンテンツセキュリティポリシー（CSP）の違反は、*report-to* または *report-uri* CSP ディレクティブを使用して事業体に報告することができます。 • CSP 自体の変更は、改ざんを示すことができます。 • 受信したウェブページを要求・解析するシステムによる外部監視（合成ユーザ監視とも呼ばれる）により、決済ページの JavaScript の変更を検出し、担当者に警告することができます 。 • 決済ページに耐タンパー性を持つ改ざん検知用スクリプトを埋め込むことで、悪意のあるスクリプトの動作を検知した場合に警告やブロックを行うことができます。 • リバースプロキシやコンテンツデリバリーネットワークにより、スクリプトの変更を検知し、担当者に警告を発することができます。 多くの場合、これらのメカニズムはサブスクリプションまたはクラウドベースですが、カスタムおよび個社開発ソリューションに基づくことも可能です。

情報セキュリティポリシーの維持

要件 12:　　組織の方針とプログラムによって情報セキュリティをサポートする

セクション
12.1 事業体の情報資産の保護について規定し、方向性を示す包括的な情報セキュリティ方針が周知され、かつ最新である。
12.2 エンドユーザ・テクノロジに関する利用規定が定義され、実施されている。
12.3 カード会員データ環境に対するリスクが正式に特定、評価、管理されている。
12.4 PCI DSS コンプライアンスを管理している。
12.5 PCI DSS の範囲が文書化され、検証されている。
12.6 セキュリティ啓発教育が継続的に行われている。
12.7 内部脅威によるリスクを低減するために、要員を選別している。
12.8 サードパーティサービスプロバイダ（TPSP）との関係に関連する情報資産へのリスクが管理されている。
12.9 サードパーティサービスプロバイダ（TPSP）は、顧客の PCI DSS 準拠をサポートする。
12.10 カード会員データ環境（CDE）に影響を及ぼす可能性のあるセキュリティインシデントが疑われる場合、または確認された場合は、直ちに対応する。

概要

組織全体の情報セキュリティ方針は、組織全体の方向性を示し、担当者に何が期待されているかを知らせるものです。すべての担当者は、カード会員データの機密性と、それを保護する責任を認識する必要があります。

要件 12 の目的では、「担当者」とは、アカウントデータを保護するセキュリティ責任を持つ、またはアカウントデータ のセキュリティに影響を与える可能性のある正社員、パートタイム社員、派遣社員、請負業者、コンサルタントを指します。

PCI DSS 用語の定義については、付録 G を参照してください。

要件とテスト手順		ガイダンス
12.1 組織の情報資産の保護を管理し、方向付ける包括的な情報セキュリティ方針が周知されており、かつ最新である。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.1.1 全体的な情報セキュリティポリシーがある。 • 確立されている。 • 発行されている。 • 維持する。 • すべての関係者および関連するベンダやビジネスパートナーに周知させる。	**12.1.1** 情報セキュリティポリシーを調査し、担当者にインタビューを行い、情報セキュリティポリシー全体が本要件で規定されたすべての要素に従って管理されていることを確認する。	組織の全体的な情報セキュリティポリシーは、カード会員データの保護を定義する他のすべてのポリシーおよび手順と関連し、これを管理します。 情報セキュリティポリシーは、カード会員データを含む最も貴重な資産の保護に関する経営陣の意図と目的を伝えるものです。 情報セキュリティポリシーがなければ、組織内で必要とされる管理について、個人が独自の価値判断を下すことになり、その結果、組織が法律、規制、契約上の義務を果たせず、一貫した方法で資産を適切に保護することができなくなる可能性があります。 ポリシーを確実に実施するためには、組織内のすべての関係者、関連する第三者、ベンダ、ビジネスパートナーに、組織の情報セキュリティポリシーと情報資産を保護する責任を認識させることが重要です。 *(次ページに続く)*
カスタマイズアプローチの目的		
情報セキュリティの戦略的目標および原則が定義され、採用され、すべての担当者に周知されている。		

要件とテスト手順		ガイダンス
		グッドプラクティス 組織のセキュリティ方針は、目的、範囲、説明責任、情報など、情報セキュリティに関する組織の立場を明確に定義するものです。 全体的な情報セキュリティ方針は、特定の技術やセキュリティ分野を扱う個々のセキュリティ方針とは異なります。このポリシーは、組織全体に対する指示を示すものであるのに対し、個々のセキュリティポリシーは、全体的なセキュリティポリシーと整合し、これを支持し、技術やセキュリティ分野の特定の目的を伝えるものです。 組織内のすべての関係者、関係する第三者、ベンダ、ビジネスパートナーは、組織の情報セキュリティポリシーと情報資産を保護する責任を認識することが重要です。 **定義** この要件における「関連」とは、情報セキュリティポリシーが、社内の、またはベンダや第三者が行うサービス／機能のために、ポリシーの一部またはすべてのトピックに該当する役割を持つ人々に普及することを意味します。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **12.1.2** 情報セキュリティポリシーは • 少なくとも 12 カ月に一度は見直す。 • 事業目的の変更または環境に対するリスクを反映させるため、必要に応じて更新する。 **カスタマイズアプローチの目的** 情報セキュリティポリシーは、組織の戦略的な目的および原則を反映し続ける事。	**定義されたアプローチのテスト手順** **12.1.2** 情報セキュリティポリシーを調査し、責任者にインタビューして、この要件で指定されたすべての要素に従ってポリシーが管理されていることを確認する。	**目的** セキュリティ上の脅威やそれに伴う防御方法は、急速に進化しています。情報セキュリティポリシーを更新し、関連する変化を反映させなければ、これらの脅威に対する新たな防御策に対処できない可能性があります。
定義されたアプローチの要件 **12.1.3** セキュリティポリシーにより、すべての担当者に対して情報セキュリティの役割と責任が明確に定義されており、すべての担当者が情報セキュリティの責任を認識し、認識している。 **カスタマイズアプローチの目的** 担当者は、事業体のカード会員データの保護における自分の役割を理解している。	**定義されたアプローチのテスト手順** **12.1.3.a** 情報セキュリティポリシーを調査し、すべての担当者に対する情報セキュリティの役割と責任を明確に定義していることを確認する。 **12.1.3.b** 様々な役割を担う担当者にインタビューを行い、彼らが情報セキュリティの責任を理解していることを確認する。 **12.1.3.c** 文書化された証拠を調査し、担当者が情報セキュリティの責任を認識していることを確認する。	**目的** セキュリティの役割が明確に定義されず、責任が明確に付与されていないと、組織の情報資産が悪用されたり、情報セキュリティ担当者とのやりとりに矛盾が生じたりして、技術の安全でない実装や時代遅れの技術や安全でない技術の使用につながる可能性があります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 十分な権限と責任を持つ者が、組織の情報セキュリティプログラムを積極的に管理し、推進するためには、組織内の幹部レベルで情報セキュリティの説明責任と責任を割り当てる必要があります。 この役割を担う一般的な経営幹部には、最高情報セキュリティ責任者（CISO）や最高セキュリティ責任者（CSO：この要件を満たすには、CSOの役割が情報セキュリティの責任者である必要があります）などがあります。これらの役職は、多くの場合、経営陣の最上位に位置し、最高経営責任者（CEO）または取締役会の直属の部下であるCレベルの役職となります。 **グッドプラクティス** また、事業者は、重要なセキュリティ活動において潜在的なギャップを回避するために、これらの主要人物の移行計画および／または後継者計画を検討すべきです。
12.1.4 情報セキュリティに関する責任が、最高情報セキュリティ責任者または情報セキュリティに精通した経営陣のメンバーに正式に割り当てられている。	**12.1.4** 情報セキュリティポリシーを調査し、情報セキュリティが最高情報セキュリティ責任者または情報セキュリティに精通した経営陣のメンバーに正式に割り当てられていることを確認する。	
カスタマイズアプローチの目的		
経営幹部が情報セキュリティの責任者として指名されている。		

要件とテスト手順		ガイダンス
12.2 エンドユーザ・テクノロジの使用に関する方針が定義され、実施されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.2.1 エンドユーザ・テクノロジに関する利用ポリシーが文書化され、実施されている。 • 権限を与えられた当事者による明示的な承認 • 技術の許容される使用方法 • 従業員が使用するために会社が承認した製品のリスト（ハードウェアとソフトウェアを含む）。	**12.2.1** エンドユーザ・テクノロジの利用規程を調査し、担当者にインタビューして、この要件で指定されているすべての要素に従ってプロセスが文書化され、実施されていることを確認する。	エンドユーザ・テクノロジは重要な投資であり、適切に管理されないと組織に大きなリスクをもたらす可能性があります。利用規定は、組織の情報技術を使用する際に担当者に期待される行動の概要を示し、組織のリスク許容度を反映させます。 これらのポリシーは、担当者が会社の機器を使ってできること、できないことを指示し、会社のインターネットや電子メールリソースの正しい使い方、間違った使い方について担当者を指導するものです。このようなポリシーは、組織を法的に保護し、ポリシーに違反した場合に対処することを可能にします。
カスタマイズアプローチの目的		**グッドプラクティス**
エンドユーザ・テクノロジの利用が定義され、許可された利用を保証するために管理されている。		利用ポリシーは、その実施の強制を管理するための技術的なコントロールによって支えられていることが重要です。 ポリシーは、目的とリンクした単純な「する」「しない」の要件として構造化することで、曖昧さをなくし、担当者に要件の背景を伝えることができます。
適用上の注意		
利用ポリシーが求められるエンドユーザ・テクノロジの例としては、リモートアクセスや無線技術、ノートパソコン、タブレット端末、携帯電話、リムーバブル電子メディア、電子メールの使用、インターネットの使用などが挙げられますが、これらに限定されない。		

要件とテスト手順		ガイダンス
12.3 カード会員データ環境に対するリスクが正式に特定、評価、管理される。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.3.1 実行頻度に柔軟性がある（たとえば、定期的に実行する要件）各 PCI DSS 要件は、文書化され、以下を含むターゲットリスク分析によってサポートされる。 • 保護対象の資産を特定する。 • 要件が保護する脅威を特定する。 • 脅威が実現する可能性および／または影響に寄与する要因の特定 • 脅威が実現する可能性を最小化するために、どの程度の頻度でその要件を実行しなければならないかを決定し、その正当性を含む分析結果。 • 少なくとも 12 カ月に一度、対象となる各リスク分析をレビューし、結果がまだ有効であるか、または最新のリスク分析が必要であるかを判断すること。 • 年次レビューで決定された通りに、必要な時期にスク分析の更新を実施。	**12.3.1** 文書化されたポリシーと手順を調べ、PCI DSS 要件ごとにターゲットリスク分析を実行するためのプロセスが定義されていること、そのプロセスがこの要件で指定されたすべての要素を含んでいることを確認する。	PCI DSS 要件の中には、環境に対するリスクに基づいてアクティビティの実行頻度を定義することを許可しているものがあります。このリスク分析を方法論に従って実行することで、有効性とポリシーおよび手順との一貫性が確保されます。 このターゲットリスク分析（従来の企業全体のリスク評価とは対照的）は、事業体が所定のコントロールを実行する頻度について柔軟性を認めている PCI DSS 要件に焦点を当てます。このリスク分析では、事業体はこの柔軟性を提供する各 PCI DSS 要件を慎重に評価し、事業体にとって適切なセキュリティをサポートする頻度と、事業体が許容するリスクレベルを決定します。 リスク分析では、要件が保護を意図するシステムコンポーネントやデータ（ログファイル、クレデンシャルなど） と、要件が資産を保護する脅威または結果（マルウェア、未検出の侵入者、クレデンシャルの誤用など）を特定します。可能性または影響に寄与する要因の例としては、脅威に対する資産の脆弱性を増大させるもの（信頼できないネットワークへのアクセス、環境の複雑さ、 *(次ページに続く)*
カスタマイズアプローチの目的		
カード会員データ環境（CDE）に対するリスクに関する最新の知識と評価が維持されている。		

要件とテスト手順		ガイダンス
適用上の注意 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		スタッフの離職率の高さ）、それに加えてシステムコンポーネントの重要性、または保護されているデータの量と機密性が含まれます。 これらのターゲットリスク分析の結果を少なくとも 12 カ月に 1 回、環境に対するリスクに影響を与える可能性のある変更時に見直すことで、組織は、リスク分析結果が組織の変更および進化する脅威、傾向、および技術に常に対応していること、および選択した頻度が依然として事業者のリスクに適切に対応していることを確認することができます。 **グッドプラクティス** 全社的なリスクアセスメントは、企業が脅威と関連する脆弱性を特定するためのポイントインタイムの活動であり、企業が事業に悪影響を及ぼす可能性のある広範かつ新たな脅威を決定し理解するために推奨されますが、必須ではありません。この全社的なリスク評価は、組織の全体的な情報セキュリティ方針の年次レビューへのインプットとして使用される、包括的なリスク管理プログラムの一部として確立することができます（要件 12.1.1 を参照）。 全社的なリスク評価のためのリスク評価手法の例としては、ISO *27005* や NIST SP *800-30* が挙げられるが、これらに限定されません。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 反復可能で堅牢な手法に従ったリスク分析により、事業者はカスタマイズアプローチの目的を達成することができます。 **定義** PCI DSS 要件を満たすためのカスタマイズアプローチでは、事業体は、定義された要件に厳密には従わない方法で、指定された要件のカスタマイズアプローチの目的を満たすために使用するコントロールを定義できます。これらのコントロールは、少なくとも定義された要件によって提供されるセキュリティを満たすかそれ以上であることが期待され、カスタマイズアプローチを使用する事業体によって広範な文書化が要求されます。 **その他の情報** カスタマイズアプローチに必要なエビデンスの文書化方法については、付録 D カスタマイズアプローチ を参照してください。 カスタマイズアプローチを文書化するために企業が使用するテンプレートについては、付録 E カスタマイズアプローチをサポートするサンプルテンプレートを参照してください。テンプレートの使用は任意ですが、各テンプレート内で指定された情報は文書化し、各事業体の評価者に提供されなければならないことに留意してください。
12.3.2 カスタマイズアプローチで事業体が満たす各 PCI DSS 要件について、以下を含むターゲットリスク分析を実施する。 • 付録 D で指定された各要素の詳細を示す文書化された証拠。カスタマイズアプローチ（最低でも、コントロールマトリクスとリスク分析を含む）で指定された各要素を詳述する文書化された証拠。 • 文書化された証拠を上級管理職が承認すること。 • 少なくとも 12 カ月に一度、ターゲットリスク分析を実施すること。	**12.3.2** カスタマイズアプローチで事業体が満たす各 PCI DSS 要件について、文書化されたターゲットリスク分析を調べ、各要件の文書が存在し、この要件で指定されたすべての要素に準拠していることを確認する。	
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの一部であり、カスタマイズアプローチを使用している場合、満たす必要がある。		
適用上の注意 この要件は、カスタマイズアプローチを使用する事業体にのみ適用される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.3.3 使用中の暗号スイートおよびプロトコルが文書化され、少なくとも 12 カ月に一度、以下のような見直しが行われる。 • 使用されているすべての暗号スイートおよびプロトコルの最新のインベントリ（目的および使用場所を含む）。 • 使用されているすべての暗号スイートとプロトコルの継続的な有効性に関して、業界の動向を積極的に監視していること。 • 暗号の脆弱性において予測される変化に対応するための文書化された戦略。	**12.3.3** 使用中の暗号スイートとプロトコルの文書を調査し、担当者にインタビューして、文書とレビューがこの要件で指定されたすべての要素に従っていることを確認する。	プロトコルや暗号強度は、脆弱性や設計上の欠陥の特定により、すぐに変更されたり、非推奨となる可能性があります。現在および将来のデータセキュリティのニーズをサポートするために、事業体は暗号が使用されている場所を知る必要があり、暗号実装の強度に影響を与える変更に迅速に対応する方法を理解する必要があります。 **グッドプラクティス** 暗号の俊敏性は、元の暗号化方式または暗号の安全性の根拠となるアルゴリズムの代替手段を確保し、システムインフラに大きな変更を加えることなく代替手段にアップグレードする計画を持つことが重要です。例えば、標準化団体によってプロトコルやアルゴリズムがいつ廃止されるかを知っていれば、廃止が運用に影響を与える前にアップグレードするための事前計画を立てることができます。 **定義** 「暗号の俊敏性」とは、組織全体に展開されている暗号化技術や関連する検証技術を監視・管理する能力のことです。 **その他の情報** *NIST SP 800-131a、暗号アルゴリズムと鍵長の使用の移行*を参照してください。
カスタマイズアプローチの目的		
事業体は、暗号プロトコルまたはアルゴリズムの脆弱性がカード会員データの保護に影響する場合、その脆弱性に迅速に対応することがでる。		
適用上の注意		
この要件は、PCI DSS 要件を満たすために使用されるすべての暗号スイートおよびプロトコルに適用される。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.3.4 使用中のハードウェアおよびソフトウェア技術について、少なくとも 12 カ月に一度、以下を含む見直しを行う。 • 当該技術が、引き続きベンダからのセキュリティ修正を速やかに受けているかどうかを分析する。 • テクノロジが引き続き事業体の PCI DSS 準拠をサポートする（妨げない）ことを分析する。 • ベンダがテクノロジの「耐用年数終了」計画を発表した場合など、テクノロジに関連する業界の発表や傾向の文書化。 • ベンダが「耐用年数終了」計画を発表したものを含め、古くなったテクノロジを修正するための、上級管理職によって承認された計画の文書化。	**12.3.4** 使用中のハードウェアおよびソフトウェア技術のレビューに関する文書を調査し、担当者にインタビューして、レビューがこの要件で指定されているすべての要素に従っていることを確認する。	ハードウェアとソフトウェアの技術は常に進化しており、組織は、ベンダや開発者によって是正されないハードウェアとソフトウェアの脆弱性に備え、管理できるように、使用する技術の変化や、それらの技術に対する脅威の進化を認識する必要があります。 **グッドプラクティス** 組織は、ファームウェアのバージョンを確認し、それらが最新であり、ベンダによってサポートされていることを確認する必要があります。また、組織は、テクノロジベンダによる製品またはプロセスの変更に注意し、そのような変更が組織のテクノロジの使用にどのような影響を及ぼす可能性があるかを理解する必要があります。 PCI DSS コントロールに影響を与える、または影響を及ぼすテクノロジを定期的にレビューすることで、購入、使用、および配備の戦略を支援し、これらのテクノロジに依存する管理が引き続き有効であることを確認することができます。これらのレビューには、ベンダのサポートが終了したテクノロジや組織のセキュリティニーズを満たさなくなったテクノロジのレビューが含まれますが、これらに限定されません。
カスタマイズアプローチの目的		
事業体のハードウェアおよびソフトウェア技術が最新のものであり、ベンダのサポートを受けています。サポートされていないすべてのシステムコンポーネントを削除または交換する計画が定期的に見直されている。		

要件とテスト手順		ガイダンス
適用上の注意		
この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
12.4 PCI DSS コンプライアンスを管理する。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.4.1 ***サービスプロバイダのみに対する追加要件:*** カード会員データの保護と PCI DSS 準拠プログラムに対する経営陣の責任が設定されており、その内容は以下のとおりです。 • PCI DSS 準拠を維持するための全体的な説明責任。 • PCI DSS 準拠を維持するための全体的な説明責任：PCI DSS 準拠プログラムに関する憲章を定義し、経営陣に伝える。	**12.4.1** ***サービスプロバイダ評価のみの追加テスト手順：*** 経営陣が、この要件で指定されたすべての要素に従って、カード会員データの保護と PCI DSS 準拠プログラムに対する責任を確立していることを確認するために文書を調査する。	経営陣による PCI DSS 準拠の責任の割り当てにより、経営陣レベルの PCI DSS 準拠プログラムへの可視性が確保され、プログラムの有効性を判断し、戦略的優先事項に影響を与えるための適切な質問をする機会が与えられます。
カスタマイズアプローチの目的		
経営幹部は、カード会員データのセキュリティに対して責任と説明責任を負う。		
適用上の注意		
経営幹部には、C レベル、取締役会、またはそれに相当する役職が含まれる場合がある。具体的な役職は、特定の組織構造によって異なる。 PCI DSS 準拠プログラムに対する責任は、個々の役割または組織内の事業単位に割り当てることができます。 この要件は、評価対象事業体がサービスプロバイダである場合にのみ適用される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
12.4.2 ***サービスプロバイダのみに対する追加要件：*** レビューは、担当者がすべてのセキュリティポリシーと運用手順に従って業務を遂行していることを確認するために、少なくとも 3 カ月に 1 回実施されます。 レビューは、所定の業務を遂行する責任者以外の担当者が実施し、以下の業務を含みますが、これに限定されません： • 日々のログレビュー • ネットワークセキュリティ制御の設定レビュー • 新規システムに対する設定基準の適用 • セキュリティアラートへの対応 • 変更管理プロセス	**12.4.2.a** ***サービスプロバイダ評価のみの追加テスト手順：*** ポリシーと手順を調査し、担当者がすべてのセキュリティポリシーとすべての運用手順（この要件で指定されたタスクを含むがこれに限定されない）に従ってタスクを実行していることを確認するためのレビューを行うためのプロセスが定義されていることを確認する。	**目的** セキュリティポリシーと手順が守られていることを定期的に確認することで、期待されるコントロールが有効であり、意図したとおりに機能していることを保証することができます。この要件は、実行すべきタスクを指定する他の要件とは異なります。これらのレビューの目的は、他の PCI DSS 要件を再実行することではなく、セキュリティ活動が継続的に実行されていることを確認することです。 **グッドプラクティス** これらのレビューは、適切なエビデンスが維持されていることを確認するためにも使用できます。たとえば、監査ログ、脆弱性スキャンレポート、ネットワークセキュリティ制御ルールセットのレビューなどは、事業体が次回の PCI DSS 評価に向けて準備する上で役に立ちます。 **例** 要件 1.2.7 を例にとると、要件 12.4.2 は、少なくとも 3 カ月に 1 回、ネットワークセキュリ ティコントロールの設定のレビューが必要な頻度で行われていることを確認することで満たされています。一方、要件 1.2.7 では、要件に規定された構成のレビューを行うことで要件を満たします。
カスタマイズアプローチの目的 重要な PCI DSS コントロールの運用の有効性を、記録の手作業による点検で定期的に確認する。	**12.4.2.b** ***サービスプロバイダ評価のみの追加試験手順：*** 担当者へのインタビューやレビューの記録を調査し、レビューが実施されていることを確認する。 • 少なくとも 3 カ月に 1 回 • 所定の業務を行う責任者以外の者が行っている。	
適用に関する注意事項 この要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.4.2.1 ***サービスプロバイダのみに対する追加要件:*** 要件 12.4.2 に従って実施されたレビューは、以下を含むように文書化されている。 • レビューの結果 • 要件 12.4.2 で実施されていないことが判明したタスクに対して実施された文書化された是正措置。 • PCI DSS コンプライアンスプログラムの責任を割り当てられた担当者による結果のレビューおよび署名。	**12.4.2.1** ***サービスプロバイダ評価のみの追加テスト手順:***PCI DSS 要件 12.4.2 に従って実施されたレビューの文書を調べ、文書にこの要件で指定されたすべての要素が含まれていることを確認する。	これらの独立したチェックの目的は、セキュリティ活動が継続的に実行されているかどうかを確認することです。これらのレビューは、適切な証拠、たとえば、監査ログ、脆弱性スキャンレポート、ネットワークセキュリティ制御ルールセットのレビューが維持されていることを確認するためにも使用でき、事業体が次回の PCI DSS 評価に向けて準備する際に役立ちます。
カスタマイズプローチの目的		
運用の有効性レビューの所見を経営陣が評価し、適切な是正活動が実施されている。		
適用に関する注意事項		
この要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用される。		

要件とテスト手順		ガイダンス
12.5 PCI DSS の適用範囲が文書化され、確認されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.5.1 機能／用途の説明を含む、PCI DSS の適用範囲にあるシステムコンポーネントのインベントリが維持され、最新の状態に保たれている。	**12.5.1.a** インベントリを調査し、適用範囲内のすべてのシステムコンポーネントとそれぞれの機能／用途の説明が含まれていることを確認する。 **12.5.1.b** インベントリが最新の状態に保たれていることを確認するため、担当者にインタビューを行う。	すべてのシステムコンポーネントの最新リストを維持することにより、組織はその環境の範囲を定義し、PCI DSS 要件を正確かつ効率的に実装することができます。インベントリがないと、一部のシステムコンポーネントが見落とされ、組織の構成基準から不注意に除外される可能性があります。 **グッドプラクティス** 企業がすべての資産のインベントリを保持する場合、PCI DSS の適用範囲にあるシステムコンポーネントは、他の資産の中で明確に識別できるようにする必要があります。 インベントリには、インスタンス化される可能性のあるコンテナまたはイメージを含める必要があります。 インベントリに所有者を割り当てることで、インベントリを最新の状態に保つことができます。 **例** インベントリを管理する方法としては、データベース、一連のファイル、インベントリ管理ツールなどがあります。
カスタマイズアプローチの目的		
PCI DSS の範囲にあるすべてのシステムコンポーネントを特定し、把握している。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
12.5.2 PCI DSS の適用範囲は、少なくとも 12 カ月に 1 回、および適用範囲内の環境に大幅な変更があった場合に、文書化され、事業体によって確認されます。最低でも、適用範囲の検確認には以下が含まれる。 • さまざまな決済段階（オーソリゼーション、キャプチャ決済、チャージバック、返金など）および受け入れチャネル（カード提示、カード非提示、電子商取引など）のすべてのデータフローを特定すること。 • 要件 1.2.4 に従って、すべてのデータフロー図を更新すること。 • アカウントデータが保存、処理、伝送されるすべての場所を特定すること（これらに限定されない。1）現在定義されているカード会員データ環境（CDE）以外の場所、2）カード会員データ（CHD）を処理するアプリケーション、3）システムおよびネットワーク間の伝送、4）ファイルのバックアップを含む。 • カード会員データ環境（CDE）内のすべてのシステムコンポーネント、カード会員データ環境（CDE）に接続されているもの、カード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるものを特定する。 *(次ページに続く)*	**12.5.2.a** 適用範囲レビューの文書化された結果を調べ、担当者にインタビューし、レビューが実施されていることを確認する。 • 少なくとも 12 カ月に一度。 • 適用範囲内の環境に大幅な変更があった場合。	**目的** PCI DSS 適用範囲の頻繁な確認は、PCI DSS 適用 範囲が常に最新で、変化するビジネス目標に一致し、その結果、セキュリティコントロールがすべての適切なシステムコンポーネントを保護していることを保証するのに役立ちます。 **グッドプラクティス** 正確な適用範囲確認には、カード会員データ環境（CDE） および接続されているすべてのシステムコンポーネントを批判的に評価し、PCI DSS 要件に必要な範囲を決定することが含まれます。慎重な分析および継続的な監視を含む適用範囲確認活動は、適用範囲内のシステムが適切に保護されていることを確認するのに役立ちます。アカウントデータの場所を文書化する場合、事業体は以下の情報を含む表またはスプレッドシートの作成を検討することができます。 • データ保存場所（データベース、ファイル、クラウドなど）、データ保存の目的、保存期間など。 • どのカード会員データ（CHD）要素が保存されているか（PAN、有効期限、カード会員名、および／またはオーソリゼーション完了前の機密認証データ（SAD）の要素）。 *(次ページに続く)*

要件とテスト手順		ガイダンス
• 使用中のすべてのセグメンテーション制御と、カード会員データ環境（CDE）がセグメンテーションされている環境（範囲外の環境の正当な理由を含む）を特定すること。 • カード会員データ環境（CDE）にアクセス可能な第三者からの全ての接続を特定すること。 • 識別されたすべてのデータフロー、アカウントデータ、システムコンポーネント、セグメンテーション制御、およびカード会員データ環境（CDE）にアクセスする第三者からの接続が範囲に含まれることを確認すること。	**12.5.2.b** 事業体が実施した適用範囲レビューの文書化された結果を調べ、PCI DSS 適用囲確認活動がこの要件で指定されたすべての要素を含んでいることを確認する。	• データの保護方法（暗号化の種類と強度、ハッシュアルゴリズムと強度、トランケーション、トークン化）。 • 使用されているログの仕組み（エンタープライズ・ソリューション、アプリケーション・レベル、オペレーティング・システム・レベルなど）の説明を含む、データ・ストアへのアクセスのログの記録方法。 内部システムおよびネットワークに加えて、ビジネスパートナー、リモートサポートサービスを提供する企業、その他のサービスプロバイダなどの第三者からのすべての接続を特定し、PCI DSS 手協範囲に含めるかどうかを判断する必要があります。適用範囲内の接続を特定したら、該当する PCI DSS コントロールを実装して、第三者接続が事業体の カード会員データ環境（CDE） を侵害するために使用されるリスクを低減することができます。データ検出ツールまたは方法を使用して、PAN のすべてのソースと場所を容易に特定し、現在定義されている カード会員データ環境（CDE） の外部のシステムおよびネットワークに存在する PAN、または定義されている カード会員データ環境（CDE） 内の予期しない場所（エラーログやメモリダンプファイルなど）に存在する PAN を検索することができます。 *(次ページに続く)*
カスタマイズアプローチの目的 PCI DSS の適用範囲は、定期的に、また大幅な変更の後に、包括的な分析と適切な技術的手段によって確認される。		
適用に関する注意事項 この PCI DSS 範囲の年次確認は、評価対象事業体が行うことが期待される活動であり、事業体の評価者が 年次評価中に行う範囲確認と同じではなく、またそれに取って代わることも意図されていない。		

要件とテスト手順		ガイダンス
		このアプローチにより、これまで知られていなかった PAN の場所が検出され、PAN が除去されるか、適切に保護されることが保証されます。 **その他の情報** その他のガイダンスについては、*情報補足: PCI DSS の適用範囲とネットワークセグメンテーションのためのガイダンス*.を参照してください。
定義されたアプローチの要件 **12.5.2.1** ***サービスプロバイダのみに対する追加要件:***PCI DSS の適用範囲は、少なくとも 6 カ月に 1 回、および適用範囲内の環境に大幅な変更があった場合に文書化され、事業体に よって確認されます。適用範囲の確認には、最低でも要件 12.5.2 で指定されたすべての要素が含まれます。 **カスタマイズアプローチの目的** 包括的な分析と適切な技術的手段により、PCI DSS 範囲の精度が継続的に高いことを確認する。	**定義されたアプローチのテスト手順** **12.5.2.1.a** ***サービスプロバイダ評価のみの追加試験手順：*** 文書化された適用範囲レビューの結果を調べ、担当者にインタビューし、要件 12.5.2 に従ったレビューが実施されていることを確認する。 • 少なくとも 6 カ月に 1 回、および • 大幅な変更の後 **12.5.2.1.b** ***サービスプロバイダ評価のみの追加テスト手順：***。適用範囲レビューの文書化された結果を調べ、適用範囲確認が要件 12.5.2 で指定されたすべての要素を含むことを確認する。	**目的** サービスプロバイダは、通常、加盟店よりも大量のカード会員データにアクセスすることができ、また、他の複数の事業体を侵害するために悪用される可能性のある入口ポイントを提供することができます。また、サービスプロバイダは通常、より大規模で複雑なネットワークを持っており、より頻繁に変更される可能性があります。サービスプロバイダの環境では、複雑で動的なネットワークで適用範囲の変更を見落とす可能性がより高くなります。

要件とテスト手順		ガイダンス
適用に関する注意事項 *この要件は、評価対象企業がサービス提供者である場合にのみ適用されます。* *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		PCI DSS の適用範囲をより頻繁に確認することで、攻撃者に悪用される前に、このような見過ごされた変更を発見できる可能性が高くなります。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.5.3 ***サービスプロバイダのみに対する追加要件：*** 組織構造の大幅な変更により、PCI DSS の範囲および管理の適用性への影響を文書化した（内部）レビューが行われ、その結果が経営陣に伝達される。	**12.5.3.a** ***サービスプロバイダ評価のみの追加テスト手順:*** ポリシーと手順を調べて、組織構造の大幅な変更により、PCI DSS の範囲とコントロールの適用性に対する影響の文書化されたレビューが行われるようなプロセスが定義されていることを確認する。	組織の構造と管理は、効果的で安全な運用のための要件とプロトコルを定義します。この構造の変更は、かつて PCI DSS のコントロールをサポートしていたリソースの再配分または削除、または確立されたコントロールがない可能性のある新しい責任の継承によって、既存のコントロールおよびフレームワークにマイナスの影響を与える可能性があります。したがって、組織の構造およびコントロールに変更があった場合は、PCI DSS の適用範囲およびコントロールを再検討して、コントロールが定められ、有効であることを確認することが重要です。
カスタマイズアプローチの目的	**12.5.3.b** ***サービスプロバイダ評価のみの追加テスト手順:*** 文書（例えば、議事録）を調査し、責任者にインタビューして、組織構造の大幅な変更が、この要件で指定されたすべての要素を含む文書化されたレビューにつながり、その結果が経営幹部に伝達されたことを確認する。	**例**
大幅な組織変更後に PCI DSS の適用範囲を確認する。		組織構造の変更には、会社の合併や買収、セキュリティコントロールに責任を持つ担当者の大幅な変更または配置転換などが含まれるが、これらに限定されません。
適用に関する注意事項		
この要件は、評価対象の事業者がサービスプロバイダである場合にのみ適用される。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
12.6 セキュリティ意識教育が継続的に実施されている。		
定義されたアプローチの要件 **12.6.1** 正式なセキュリティ意識向上プログラムが実施され、すべての担当者に組織の情報セキュリティポリシーと手順、およびカード会員データの保護における各自の役割を認識させる。 **カスタマイズアプローチの目的** 担当者は、脅威の状況、関連するセキュリティ管理の運用に対する責任について知識があり、必要に応じて支援や指導にアクセスすることができる。	**定義されたアプローチのテスト手順** **12.6.1** セキュリティ啓蒙プログラムを調査し、組織の情報セキュリティポリシーと手順、およびカード会員データの保護における担当者の役割について、すべての担当者に啓蒙していることを確認する。	**目的** 担当者が、自社の情報セキュリティ方針と手順、および各自のセキュリティ責任について教育を受けていない場合、意図しないエラーや意図的な行動によって、導入済みのセキュリティ保護策やプロセスが効果を失う可能性があります。
定義されたアプローチの要件 **12.6.2** セキュリティ啓発プログラムは • 少なくとも 12 カ月に 1 回見直す。 • 事業体の カード会員データ環境（CDE） のセキュリティに影響を与える可能性のある新しい脅威および脆弱性、またはカード会 員データの保護における役割について担当者に提供される情報に対処するために、必要に応じて更新 する。 **カスタマイズアプローチの目的** セキュリティ啓発資料の内容が定期的に見直され、更新されている。	**定義されたアプローチのテスト手順** **12.6.2** セキュリティ啓発プログラムの内容、レビューの証拠を調査し、担当者にインタビューして、セキュリティ啓発プログラムがこの要件で指定されたすべての要素に準拠していることを確認する。	**目的** 脅威の環境と企業の防御は静的なものではありません。従って、セキュリティ啓発プログラムの資料は、担当者が受ける教育が最新のものであり、現在の脅威環境を表していることを保証するために、必要に応じて頻繁に更新されなければなりません。

要件とテスト手順		ガイダンス
適用に関する注意事項 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		
定義されたアプローチの要件 **12.6.3** 担当者は、以下のようにセキュリティ意識向上トレーニングを受ける。 • 入社時、および少なくとも 12 カ月に 1 回。 • 複数のコミュニケーション手段を用いる。 • 従業員は、情報セキュリティ方針および手順を読み、理解したことを少なくとも 12 カ月に 1 度、同意する。	**定義されたアプローチのテスト手順** **12.6.3.a** セキュリティ啓発プログラムの記録を調べ、担当者が入社時および 12 カ月に 1 回以上の頻度でセキュリティ啓発トレーニングを受講していることを確認する。 **12.6.3.b** セキュリティ啓発プログラムの資料を調べ、プログラムに啓発の伝達と教育を行う複数の方法が含まれていることを確認する。 **12.6.3.c** 担当者にインタビューし、意識向上トレーニングを完了し、カード会員データの保護における自分の役割を認識し ていることを確認する。 **12.6.3.d** セキュリティ啓発プログラムの資料と担当者の確認書を調査し、担当者が情報セキュリティポリシーと手順を読み、理解したことを少なくとも 12 カ月に一度は同意していることを確認する。	**目的** 担当者のトレーニングは、情報セキュリティの重要性に関する情報を確実に伝達し、組織を守るための自らの役割を理解させるものです。 また、担当者がセキュリティポリシーと手順を読み、理解したこと、およびこれらのポリシーを順守することを約束し、今後も約束することを確認するために、担当者による同意書を要求することが有効です。 **グッドプラクティス** 企業は、人事の新規採用人材の受け入れプロセスの一環として、新入社員研修を取り入れることができます。研修では、セキュリティ関連の「すべきこと」と「すべきでないこと」の概要を説明します。 定期的な再教育により、忘れられたり回避されたりする可能性のある重要なセキュリティ・プロセスや手順を強化します。 *(次ページに続く)*
カスタマイズアプローチの目的 従業員が、脅威の状況、関連するセキュリティ管理の運用に対する各自の責任に関する知識を維持し、必要なときに支援や指導にアクセスすることが可能である。		

要件とテスト手順		ガイダンス
		アカウントデータのセキュリティに影響を与える可能性のある担当者に、これまで影響を与えなかった担当者が異動する場合は、常にセキュリティ意識向上トレーニングを義務付けることを検討する必要があります。 トレーニングの方法と内容は、担当者の役割によって異なる可能性があります。 **例** ポスター、手紙、ウェブ ベースのトレーニング、対面式トレーニング、チームミーティング、インセンティブなど、セキュリティ意識と教育を提供するために使用できるさまざまな方法があります。 従業員の同意は、文書または電子的に記録することができます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.6.3.1 セキュリティ意識向上トレーニングには、カード会員データ環境（CDE）のセキュリティに影響を与える可能性のある脅威や脆弱性についての意識が含まれている。 • フィッシングおよび関連する攻撃 • ソーシャル・エンジニアリング	**12.6.3.1** セキュリティ啓発研修の内容を調査し、この要件で指定されているすべての要素が含まれていることを確認する。	フィッシングや関連する攻撃、ソーシャル・エンジニアリングの試みを検知し、対処し、報告する方法について担当者を教育することは、攻撃の成功確率を最小化するために不可欠です。 **グッドプラクティス** 効果的なセキュリティ啓発プログラムには、フィッシングメールの例や、そのような攻撃を報告する担当者の普及率を調べるための定期的なテストが含まれている必要があります。このトピックに関するトレーニング教材としては、以下のようなものが考えられます。 • フィッシングやその他のソーシャル・エンジニアリング攻撃の見分け方 • フィッシングやソーシャル・エンジニアリングの疑いがある場合の対処方法。 • フィッシングやソーシャル・エンジニアリングの疑いのある行為を報告する場所と方法。 報告を重視することで、組織は積極的な行動に報いることができ、技術的防御を最適化し（要件 5.4.1 を参照）、技術的防御を回避した同様のフィッシングメールを受信者の受信トレイから削除する措置を直ちに講じることができます。
カスタマイズアプローチの目的		
担当者は、自分自身の人間的な脆弱性と、脅威者がどのようにその脆弱性を利用しようとするかについて知識を有しています。担当者は、必要に応じて支援やガイダンスにアクセスすることができる。		
適用に関する注意事項		
フィッシング攻撃を検知し、ユーザを保護するための技術的コントロールと自動化コントロールの違いに関するガイダンスについては要件 5.4.1 を、フィッシングとソーシャルエンジニアリングに関するセキュリティ啓発トレーニングをユーザに提供するための本要件を参照する事。これらは 2 つの独立した要件であり、一方の要件は、他方の要件で要求される管理策を実施することで満たされるものではない。 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。*		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.6.3.2 セキュリティ啓発トレーニングには、要件 12.2.1 に従って、エンドユーザ・テクノロジの許容される使用に関する啓発が含まれる。	**12.6.3.2** セキュリティ啓発研修の内容を調査し、要件 12.2.1 に従ってエンドユーザ・テクノロジの許容される使用に関する啓発が含まれていることを確認する。	使用ポリシーのキーポイントを定期的なトレーニングおよび関連する文脈に含めることにより、担当者は自分の責任とそれが組織のシステムのセキュリティにどのように影響するかを理解することができます。
カスタマイズアプローチの目的		
担当者は、エンドユーザ・テクノロジのセキュリティおよび運用に関する責任について知識があり、必要なときに支援および指導にアクセスすることができる。		
適用に関する注意事項		
この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		

要件とテスト手順		ガイダンス
12.7 内部脅威によるリスクを低減するために、担当者のスクリーニングを行う。		
定義されたアプローチの要件 **12.7.1** カード会員データ環境（CDE）にアクセスする可能性のある担当者は、現地法の制約の範囲内で、雇用前にスクリーニングされ、内部情報源からの攻撃のリスクを最小化することができる。 **カスタマイズアプローチの目的** 新しいスタッフにカード会員データ環境（CDE）へのアクセスを許可することに関するリスクが理解され、管理されている。 **適用に関する注意事項** 店舗のレジ係など、取引を円滑に進めるために一度に 1 つのカード番号にしかアクセスでき ないポジションに採用される可能性のある担当者については、この要件は推奨事項のみである。	**定義されたアプローチのテスト手順** **12.7.1** カード会員データ環境（CDE）にアクセスする可能性のある潜在的な担当者を採用する前に、現地法の制約の範囲内でスクリーニングが実施されていることを確認するために、担当の人事部門管理者にインタビューする。	**目的** カード会員データ環境（CDE）にアクセスすることが予想される潜在的な担当者を雇用する前に徹底したスクリーニングを行うことで、カード会員データ環境（CDE）にアクセスすることになる雇用する担当者について、十分な情報に基づいたリスク決定を行うために必要な情報を事業体に提供します。 その他にも、職場の安全確保や、履歴書に記載された情報の確認など、潜在的な人材のスクリーニングの利点があります。 **グッドプラクティス** 事業体は、既存の従業員がカード会員データ環境（CDE）にアクセスできない職務からアクセスできる職務に異動する場合は、いつでもスクリーニングを検討する必要があります。 効果的であるためには、スクリーニングのレベルは、その職務に適切でなければなりません。例えば、より大きな責任を必要とする役職や、重要なデータやシステムへの管理アクセスを持つ役職は、責任やアクセスの少ない役職よりも、より詳細な、またはより頻繁なスクリーニングが必要となる場合があります。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		例 スクリーニングの選択肢には、企業の地域に応じて、過去の雇用履歴、公開情報／ソーシャルメディアリソースのレ ビュー、犯罪歴、信用履歴、リファレンスチェックを含めることができます。

要件とテスト手順		ガイダンス
12.8 サードパーティサービスプロバイダ（TPSP）との関係に関連する情報資産へのリスクが管理されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.8.1 アカウントデータを共有している、またはアカウントデータのセキュリティに影響を与える可能性のあるサードパーティサービスプロバイダ（TPSP）の全リスト（提供するサービスごとの説明を含む）を維持する。	**12.8.1.a** ポリシーおよび手続を調査し、アカウントデータが共有される、またはアカウントデータのセキュリティに影響を与える可能性のある全ての TPSP について、提供されるサービスごとの説明を含む TPSP のリストを維持するためのプロセスが定義されていることを確認する。	すべての TPSP のリストを維持することにより、潜在的なリスクが組織の外部に及ぶ場所を特定し、組織の拡大した攻撃対象領域を定義することができます。 **例** TPSP の種類には、以下のようなものがあります。 • 決済ゲートウェイ、決済プロセッサー、決済サービスプロバイダ（PSP）、オフサイトストレージプロバイダなど、事業体に代わってアカウントデータを保存、処理、または送信する。 • 事業体の PCI DSS 評価に含まれるシステムコンポーネントを管理する（ネットワークセキュリティ制御サービス、マルウェア対策サービス、セキュリティインシデントおよびイベント管理（SIEM）のプロバイダ、コンタクトおよびコールセンター、ウェブホスティング会社、IaaS、PaaS、SaaS、FaaS クラウドプロバイダなど）。 • 事業体のカード会員データ環境（CDE）のセキュリティに影響を与える可能性がある（リモートアクセスでサポートを提供するベンダ、特注ソフトウェア開発者等）。
カスタマイズアプローチの目的	**12.8.1.b** 文書を調査し、すべての TPSP のリストが、提供されるサービスの説明を含んで維持されていることを確認する。	
TPSP と提供されるサービスに関する記録が維持されている。		
適用に関する注意事項		
PCI DSS 準拠の TPSP を使用することによって、事業体が PCI DSS 準拠になるわけではなく、また、事業体自身の PCI DSS 準拠に対する責任がなくなるわけではない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.8.2 TPSP との契約書は、以下のように維持されている。 • アカウントデータを共有する、またはカード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるすべての TPSP との間で、書面による同意を維持する。 • 書面による同意には、TPSP が所有するアカウントデータ、または事業体のために保存、処理、伝送するアカウントデータ、または事業体のカード会員データ環境（CDE）のセキュリティに影響を与える可能性のある範囲について、TPSP が責任を負うという TPSP からの確認が含まれている。	**12.8.2.a** ポリシーと手順を調査し、本要件で指定されたすべての要素に従って、すべての TPSP との書面による同意を維持するためのプロセスが定義されていることを確認する。	TPSP の書面による同意は、TPSP が顧客から取得するアカウントデータの適切なセキュリティを維持すること、および TPSP のサービスのプロビジョニング中に影響を受ける可能性のある資産を十分に認識していることを示すものです。特定の TPSP がアカウントデータのセキュリティにどの程度責任を持つかは、提供されるサービスおよび提供者と評価対象企業（顧客）との間の契約によって異なります。 要件 12.9.1 と共に、この要件は、適用される PCI DSS 責任に関する当事者間の一貫したレベルの理解を促進することを意図しています。たとえば、提供されるサービスの一部として維持されるべき該当する PCI DSS 要件を契約に含めることができます。
カスタマイズアプローチの目的	**12.8.2.b** TPSP との書面による同意が、本要件で規定されるすべての要素に従って維持されていることを確認する。	**グッドプラクティス**
各 TPSP がアカウントデータを保護する責任について同意した記録を維持している。		また、事業体は、TPSP が要件 12.9.2 に従った事業体の情報要求をサポートすることを TPSP との契約書に含めることを検討したいかもしれません。また、事業体は、TPSP が他の TPSP と「ネストした」関係（プライマリ TPSP がサービス提供のために他の TPSP と契約すること）になっていないかどうかを把握したいでしょう。
適用に関する注意事項		
謝辞の正確な文言は、両当事者の同意、提供されるサービスの詳細、および各当事者に割り当てられた責任に依存する。謝辞は、この要件で提供される正確な文言を含む必要はない。		
(次ページに続く)		*(次ページに続く)*

要件とテスト手順		ガイダンス
TPSP が PCI DSS 要件を満たしている証拠（たとえば、PCI DSS コンプライアンスに関する証明書（AOC）や企業の ウェブサイト上の宣言）は、この要件で指定されている書面による契約書と同じものではない。		プライマリ TPSP が、サービス全体のコンプライアンスを達成するためにセカンダリ TPSP に依存しているかどうか、また、プライマリ TPSP がセカンダリ TPSP とどのような種類の書面契約を締結しているかを把握することが重要です。事業者は、プライマリ TPSP が使用する「ネストされた」TPSP に対する補償を契約書に含めることを検討することができます。 **その他の情報** 詳細なガイダンスは、*「情報補足：サードパーティセキュリティ保証」*をご参照ください。
定義されたアプローチの要件 **12.8.3** TPSP との契約前の適切なデューディリジェンスを含む、TPSP を契約するための確立されたプロセスが実施されている。	**定義されたアプローチのテスト手順** **12.8.3.a** ポリシーと手続きを調査し、契約前の適切なデューディリジェンスを含め、TPSP を契約するためのプロセスが定義されていることを確認する。	**目的** TPSP との正式な関係を構築する前に、TPSP が事業体内部で十分に吟味され、TPSP との契約に伴うカード会員データへのリスクが理解されるように、契約前の選定や審査の詳細を含む TPSP との契約プロセスを徹底することが有効です。
	12.8.3.b TPSP を契約するためのプロセスに、契約前の適切なデューディリジェンスが含まれていることを確認するために、証拠を調査し、担当者にインタビューする。	**グッドプラクティス** 具体的なデューデリジェンスのプロセスや目標は、各組織によって異なります。 考慮すべき要素には、プロバイダの報告方法、違反通知およびインシデント対応手順、各当事者間で PCI DSS 責任がどのように割り当てられるかの詳細、TPSP が自らの PCI DSS 準拠を検証する方法、およびプロバイダが提供するエビデンスが含まれます。
カスタマイズアプローチの目的 アカウントデータを適切に保護するための TPSP 候補の能力、意図、およびリソースが、TPSP と契約する前に評価される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 契約しているすべての TPSP の PCI DSS 準拠状況を把握することで、TPSP が組織に提供するサービスに適用される要件に準拠しているかどうかを保証および認識することができます。 **グッドプラクティス** TPSP がさまざまなサービスを提供している場合、事業体が監視する準拠状況は、事業体に提供されるサービスおよび事業体の PCI DSS 評価の適用範囲のサービスに特定する必要があります。 TPSP が PCI DSS 準拠の証明書（AOC）を所有している場合、TPSP は要求に応じてそれを顧客に提供し、PCI DSS 準拠状態を証明することが期待されます。 TPSP が PCI DSS 評価を受けていない場合、正式な準拠確認を受けることなく、適用される要件を満たしていることを示す他の十分な証拠を提供することができる場合があります。たとえば、TPSP は事業体の評価者に特定の証拠を提供して、評価者が該当する要件が満たされていることを確認できるようにすることができます。あるいは、TPSP は、各顧客の評価者による複数のオンデマンド評価を受けることを選択でき、 *(次ページに続く)*
12.8.4 TPSP の PCI DSS 準拠状況を少なくとも 12 カ月に 1 度監視するプログラムが導入されている。	**12.8.4.a** ポリシーと手順を調査し、TPSP の PCI DSS 準拠状況を少なくとも 12 カ月に 1 回監視するためのプロセスが定義されていることを確認する。	
	12.8.4.b 文書を調査し、担当者にインタビューして、各 TPSP の PCI DSS 準拠状況が少なくとも 12 カ月に 1 回監視されていることを確認する。	
カスタマイズアプローチの目的		
TPSP の PCI DSS 準拠状況を定期的に確認している。		
適用に関する注意事項		
事業体が、事業体に代わって PCI DSS 要件を満たすために TPSP と契約している場合（たとえば、ファイアウォールサービスを介する）、事業体は TPSP と協力して、該当する PCI DSS 要件が満たされていることを確認する必要がある。TPSP が該当する PCI DSS 要件を満たしていない場合、その事業体についても、それらの要件は「未対応」になる。		

要件とテスト手順		ガイダンス
		各評価は適用される要件が満たされていることを確認することを目標とします。 **その他の情報** サードパーティサービスプロバイダの詳細については、以下を参照してください。 • PCI DSS のセクション：サードパーティサービスプロバイダの使用 • *情報補足：サードパーティセキュリティ保証*
定義されたアプローチの要件 **12.8.5** どの PCI DSS 要件が各 TPSP によって管理され、どれが事業体によって管理され、TPSP と事業体の間で共有されている要件かについての情報が保持される。 **カスタマイズアプローチの目的** 各 TPSP が単独または共同で責任を負う PCI DSS 要件および関連するシステムコンポーネントの詳細を記した記録を維持し、定期的にレビューする。	**定義されたアプローチのテスト手順** **12.8.5.a** ポリシーと手順を調べて、どの PCI DSS 要件が各 TPSP によって管理され、どれが事業体によって管理され、どれが TPSP と事業体の両方で共有されているかについての情報を維持するためのプロセスが定義されていることを確認する。 **12.8.5.b** 文書を調査し、担当者にインタビューして、どの PCI DSS 要件が各 TPSP によって管理され、どれが事業体によって管理され、どれが両事業体間で共有されているかについての情報を事業体が保持していることを確認する。	**目的** 事業体は、TPSP が満たすことに同意した PCI DSS 要件および下位要件、TPSP と事業体の間で共有される要件、共有される要件については、要件の共有方法と各要件を満たす責任がある事業体に関する詳細を理解することが重要です。 このような共通の理解がない場合、事業体および TPSP が特定の PCI DSS 要件を相手側の責任と見なし、その 要件がまったく対処されない可能性があります。 事業体が維持する特定の情報は、プロバイダとの特定の契約、サービスの種類などに依存します。TPSP は、 *(次ページに続く)*

要件とテスト手順		ガイダンス
		自社の PCI DSS 責任をすべての顧客に対して同じであると定義することができますが、そうでない場合は、この責任につい ては、事業体および TPSP の両方が合意する必要があります。 **グッドプラクティス** 事業体は、適用されるすべての PCI DSS 要件を特定し、各要件について、その要件を満たす責任が事業体または TPSP のいずれにあるのか、または共有責任であるかを示すマトリックスを通じて、これらの責任を文書化することができます。この種の文書は、*責任マトリックス*と呼ばれることがよくあります。 また、事業体は、TPSP が他の TPSP と「ネスト型」関係（プライマリ TPSP がサービス提供のために他の TPSP と契約している・入れ子の関係）にあるかどうかを理解することも重要です。プライマリ TPSP がセカンダリ TPSP に依存してサービス全体の準拠を達成しているかどうか、およびプライマリ TPSP がサービスのパフォーマンスとセカンダリ TPSP の PCI DSS 準拠状況をどのように監視しているかを理解することが重要です。セカンダリ TPSP を管理および監視するのはプライマリ TPSP の責任であることに注意してください。 *(次ページに続く)*

要件とテスト手順		ガイダンス
		その他の情報 *情報補足：サードパーティセキュリティ保証責任マトリックステンプレートのサンプル*

要件とテスト手順		ガイダンス
12.9 サードパーティサービスプロバイダ（TPSP）は、その顧客の PCI DSS 準拠をサポートします。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.9.1 ***サービスプロバイダのみに対する追加要件：*** TPSP は、TPSP が保有する、または顧客に代わって保存、処理、伝送するアカウントデータのセキュリティ、または顧客のカード会員データ環境（CDE）のセキュリティに影響を与える可能性がある範囲について、顧客が責任を負うことを認める内容の顧客に書面による契約を維持する。	**12.9.1** ***サービスプロバイダ評価のみの追加テスト手順：*** TPSP のポリシー、手順、および契約書に使用されるテンプレートを調査し、TPSP が本要件で指定されたすべての要素に従って顧客に書面で確認書を提供するためのプロセスが定義されていることを確認する。	要件 12.8.2 と併せて、この要件は、適用される PCI DSS 責任について TPSP とその顧客の間で一貫したレベルの理解を促進することを意図しています。TPSP の同意は、TPSP が顧客から取得するアカウントデータの適切なセキュリティを維持することに対する TPSP のコミットメントを証明するものです。 TPSP が書面による同意書を提供する方法は、プロバイダとその顧客の間で合意する必要があります。
カスタマイズアプローチの目的		
TPSP は、顧客に対して、セキュリティに関する責任を正式に同意する。		
適用に関する注意事項		
同意の正確な文言は、両当事者の合意、提供されるサービスの詳細、および各当事者に割り当てられた責任に依存する。同意は、この要件で提供される正確な文言を含む必要はない。 この要件は、評価対象の事業体がサービスプロバイダである場合にのみ適用される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.9.2 ***サービスプロバイダのみに対する追加要件：*** TPSP は、要件 12.8.4 および 12.8.5 を満たすために、顧客の要求に応じて以下を提供することにより、顧客の情報開示要求をサポートするものとする。 • TPSP が顧客に代わって実行するあらゆるサービスに関する PCI DSS 準拠状況情報（要件 12.8.4）。 • どの PCI DSS 要件が TPSP の責任であり、どれが顧客の責任であるかに関する情報（共有責任を含む）（要件 12.8.5）。	**12.9.2** ***サービスプロバイダ評価のみの追加テスト手順:*** TPSP は、顧客の情報要求をサポートするためのプロセスが、要件 12.8.4 および 12.8.5 を満たすために、この要件で規定されているすべての要素に従って定義されていることを確認するために、ポリシーおよび手順を確認する。	TPSP が、顧客がセキュリティおよびコンプライアンス要件を満たすために必要な情報を提供しない場合、顧客はカード会員データを保護することができず、自らの契約上の義務も果たすことができません。
カスタマイズアプローチの目的		**グッドプラクティス**
TPSP は、顧客の PCI DSS 準拠の取り組みを支援するために、必要に応じて情報を提供する。		TPSP が PCI DSS 準拠の証明書（AOC）を所有している場合、TPSP は要求に応じてそれを顧客に提供し、PCI DSS 準拠状態を証明することが期待されます。 TPSP が PCI DSS 評価を受けていない場合は、正式な準拠確認を受けることなく、適用される要件を満たしていることを示す他の十分な証拠を提供できる可能性があります。たとえば、TPSP は事業体の評価者に特定の証拠を提供して、評価者が該当する要件が満たされていることを確認できるようにすることができます。あるいは、TPSP は、各顧客の評価者による複数のオンデマンド評価を受けることを選択でき、それぞれの評価は適用される要件が満たされていることを確認することを目標とします。 TPSP は、TPSP の PCI DSS 評価の範囲が顧客に適用されるサービスを対象としており、関連する PCI DSS 要件が調査され、実施されていると判断されたことを確認するための十分な証拠をその顧客に提供する必要があります。
適用に関する注意事項		
この要件は、評価対象の事業者がサービスプロバイダである場合にのみ適用される。		

要件とテスト手順		ガイダンス
		TPSP は、その PCI DSS 責任をすべての顧客に対して同じであると定義するか、またはこの責任は顧客と TPSP の双方で合意する必要があります。顧客は、TPSP が満たすことに同意した PCI DSS 要件およびサブ要件、TPSP と顧客の間で共有される要件、および共有される要件については、その共有方法と各サブ要件を満たす責任を負う事業体についての詳細を理解することが重要です。これらの責任を文書化する方法の例としては、該当するすべての PCI DSS 要件を特定し、その要件を満たす責任が顧客または TPSP にあるか、共有責任であるかを示すマトリックスを使用することが挙げられます。 **その他の情報** 詳細なガイダンスについては、以下を参照してください。 • PCI DSS のセクション：*サードパーティサービスプロバイダの使用* • 情報補足：サードパーティセキュリティ保証 (責任マトリックステンプレートのサンプルを含む)。

要件とテスト手順		ガイダンス
12.10 カード会員データ環境（CDE）に影響を与える可能性のあるセキュリティインシデントの疑いおよび確認されたインシデントに即座に対応する。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.10.1 インシデント対応計画が存在し、セキュリティインシデントの疑いまたは確認があった場合に発動できる状態になっている。この計画には、以下が含まれるが、これらに限定されない。 • 少なくとも、ペイメントブランドおよびアクワイアラへの通知を含む、セキュリティインシデントが発生した場合 の役割、責任、連絡および問い合わせ戦略。 • インシデントの種類に応じた特定の封じ込めおよび低減活動を伴うインシデント対応手順。 • ビジネスの復旧と継続のための手順 • データバックアッププロセス • 侵害の報告に関する法的要件の分析 • すべての重要なシステムコンポーネントの範囲と対応。 • ペイメントブランドによるインシデント対応手順の参照または包含	**12.10.1.a** インシデント対応計画を調査し、計画が存在し、少なくともこの要件で指定された要素が含まれていることを確認する。 **12.10.1.b** 担当者にインタビューし、過去に報告されたインシデントまたはアラートの文書を調査し、文書化されたインシデント対応計画および手順が順守されていることを確認する。	責任を持つ関係者に適切に周知され、読まれ、理解されている包括的なインシデント対応計画がなければ、混乱と統一された対応の欠如により、事業のダウンタイムがさらに長くなり、公共メディアへの不要な公開、財務上および／または評判の損失や法的責任のリスクを生じさせる可能性があります。 **グッドプラクティス** インシデント対応計画は、アカウントデータに影響を与える可能性のある侵害が発生した場合に、事業体が効果的に対応できるように、関係者（例えば、法務、広報）にとって重要な要素をすべて含む徹底したものでなければなりません。この計画には、インシデント対応に役割を果たすと指定されたすべての個人の最新の連絡先を記載しておくことが重要です。通知の対象となるその他の関係者には、顧客、金融機関（アクワイアラおよびイシュア）、およびビジネス・パートナーが含まれる場合があります。 事業者は、アカウントデータ、無線暗号化キー、アカウントデータまたはカード会員データの伝送および保存に使用される暗号化キーなどを含む、カード会員データ環境（CDE）内のデータのすべ
カスタマイズアプローチの目的		
カードブランドの期待に応える包括的なインシデント対応計画が維持されている。		

要件とテスト手順		ガイダンス
		ての侵害に対処する方法をインシデント対応計画で考慮する必要があります。 **例** 危殆化の報告に関する法的要件には、米国のほとんどの州、EU 一般データ保護規則（GDPR）、個人データ保護法（シンガポール）などがあります。 **その他の情報** 詳しくは、*NIST SP 800-61 改訂 2 版 コンピュータセキュリティインシデント対応ガイド*を参照してください。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.10.2 少なくとも 12 カ月に一度、セキュリティインシデント対応計画は、 • 見直され、必要に応じて内容が更新される。 • 要件 12.10.1 に記載されているすべての要素を含めてテストされている。	**12.10.2** 担当者にインタビューし、文書をレビューして、少なくとも 12 カ月に一度、セキュリティインシデント対応計画が以下であることを確認する。 • 必要に応じて見直され、更新される。 • 要件 12.10.1 に記載されているすべての要素を含めてテストされている。	セキュリティインシデント対応計画の適切なテストにより、破綻したビジネスプロセスを特定し、重要なステップを見逃さないようにすることで、インシデント発生時の漏洩を増大させる可能性を検知することができます。計画の定期的なテストは、プロセスが実行可能であり続けることを保証

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 インシデント対応計画が最新の状態に保たれ、定期的にテストされていること。		するとともに、組織内のすべての関係者が計画に精通していることを確実にします。 **グッドプラクティス** インシデント対応計画のテストには、関係者が参加する「机上訓練」の形で、インシデントのシミュレーションと対応策を含めることができます。インシデントおよび対応の品質のレビューは、すべての要求される要素が計画に含まれているという保証を事業体に提供することができます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.10.3 セキュリティインシデントの疑いまたは確認に対応するため、24 時間 365 日対応可能な担当者が指定されている。	**12.10.3** 文書を調査し、指定された役割を担う責任者にインタビューを行い、特定の担当者がセキュリティインシデントに対応するために 24 時間 365 日体制が可能なように指名されていることを確認する。	インシデントはいつでも発生する可能性があるため、インシデント対応の訓練を受け、事業体の計画に精通している者がインシデントを検知したときに対応できれば、事業体がインシデントに正しく対応する能力が高まることになります。 **グッドプラクティス** 多くの場合、セキュリティインシデント対応チームの一員として特定の担当者が指名され、インシデントへの対応（おそらく輪番制）および計画に従ってインシデントを管理する全体的な責任を担います。インシデント対応チームは、恒久的に配置されるコア・メンバー、または専門知識とインシデントの詳細に応じて必要に応じて招集される「オンデマンド」担当者で構成することができます。 インシデントに迅速に対応するために利用可能なリソースを持つことで、組織の混乱を最小限に抑えることができます。 チームまたは個人が対応すべき活動の種類には、不正な活動の証拠、不正な無線アクセスポイントの検出、重要な IDS 警告、不正な重要システムまたはコンテンツファイルの変更に関するレポートなどが含まれます。
カスタマイズアプローチの目的		
インシデントは、適切な場合には直ちに対応される。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **12.10.4** セキュリティインシデントの疑いおよび確認に対応する担当者は、インシデント対応の責任について適切かつ定期的に訓練を受ける。 **カスタマイズアプローチの目的** 担当者は、インシデント対応における自分の役割と責任について知識があり、必要なときに支援と指導を受けることができる。	**定義されたアプローチのテスト手順** **12.10.4** トレーニング文書を調査し、インシデント対応担当者にインタビューし、担当者がインシデント対応責任について適切かつ定期的にトレーニングを受けていることを確認する。	**目的** 訓練され、すぐに対応できるインシデント対応チームがなければ、ネットワークへのダメージが拡大し、標的とされたシステムの不適切な処理によって重要なデータやシステムが「汚染」される可能性があります。これは、インシデント発生後の調査の成功を妨げることになりかねません。 **グッドプラクティス** インシデント対応に携わるすべての担当者が、フォレンジックや調査のための証拠管理に関する訓練と知識を身につけることが重要です。
定義されたアプローチの要件 **12.10.4.1** インシデント対応担当者の定期的な訓練の頻度は、要件 12.3.1 に規定されたすべての要素に従って実施される、事業体の目標リスク分析で定義される。 **カスタマイズアプローチの目的** インシデント対応担当者は、事業者のリスクに対応した頻度で訓練を受けている。 **適用に関する注意事項** *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に考慮する必要がある。*	**定義されたアプローチのテスト手順** **12.10.4.1.a** インシデント対応担当者の訓練頻度について、事業体の目標を定めたリスク分析を調べ、リスク分析が要件 12.3.1 に規定されるすべての要素に従って実施されたことを確認する。 **12.10.4.1.b** インシデント対応担当者の定期的な訓練の文書化された結果を調査し、担当者にインタビューして、この要件のために実施した事業体の目標を定めたリスク分析で定義された頻度で訓練が実施されていることを確認する。	**目的** 各事業体の環境やインシデント対応計画はそれぞれ異なり、そのアプローチは、事業体の規模や複雑さ、環境の変化の度合い、インシデント対応チームの規模、担当者の入れ替わりなど、様々な要因に左右されます。 リスク分析を行うことで、事業体は、インシデント対応に責任を持つ担当者の訓練の最適な頻度を決定することができます。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.10.5 セキュリティインシデント対応計画には、セキュリティ監視システムからのアラートの監視と対応が含まれるが、これらに限定されない。 • 侵入検知システムおよび侵入防止システム。 • ネットワークセキュリティ管理 • 重要ファイルの変更検出メカニズム。 • 決済ページの変更および改ざん検知メカニズム。*この箇条は、発効日までのベストプラクティスである。詳細については、以下の適用上の注意を参照のこと。* • 未許可の無線アクセスポイントの検出。	**12.10.5** 文書を調査し、インシデント対応プロセスを観察して、セキュリティ監視システムからのアラートの監視と対応が、この要件で指定されたシステムを含むがこれに限定されない、セキュリティインシデント対応計画の対象になっていることを確認する。	データに対する潜在的なリスクに焦点を当てるよう明確に設計されたセキュリティ監視システムによって生成されたアラートに対応することは、侵害を防ぐために重要であるため、インシデント対応プロセスに含まれなければなりません。
カスタマイズアプローチの目的		
監視・検知技術によって発生したアラートに対して、構造化された反復可能な方法で対応している。		
適用に関する注意事項		
上記の項目（ペイメントページの変更および改ざん検出メカニズムからのアラートの監視と対応）は、2025 年 3 月 31 日まではベストプラクティスである。2025 年 3 月 31 日以降は要件 12.10.5 の一部として要求され、PCI DSS 評価中に十分に考慮する必要がある。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.10.6 セキュリティインシデント対応計画は、得られた教訓を踏まえて、また業界の動向を組み込み変更および改善する。	**12.10.6.a** ポリシーと手順を調査し、教訓に従ってセキュリティインシデント対応計画を変更し改善させ、業界の動向を取り入れるためのプロセスが定義されていることを確認する。	インシデント後に、業界の動向に合わせて「得られた教訓」をインシデント対応計画に教訓を組み込むことで、計画を最新状態に保ち、新たな脅威やセキュリティの傾向に対応することができるようになります。
カスタマイズアプローチの目的	**12.10.6.b** セキュリティインシデント対応計画を調査し、担当者にインタビューすることで、インシデント対応計画が、学んだ教訓に従って、また業界の発展を取り入れるために修正され、発展していることを確認する。	**グッドプラクティス**
インシデント対応計画の有効性・正確性を見直し、発動の都度更新している。		教訓を得るための演習は、すべてのレベルの担当者が参加する必要があります。インシデント全体のレビューの一部として含まれることが多いですが、インシデントに対する事業体の対応がどのように改善され得るかに焦点を当てる必要があります。 計画通りの結果が得られなかった対応の要素だけを検討するのではなく、何がうまくいったのか、うまくいった要素の教訓を計画のうまくいかなかった部分に生かせるかどうかを理解することが重要です。 事業体のインシデント対応計画を最適化するもう一つの方法は、他の組織に対する攻撃を理解し、その情報を使って事業体の検知、抑制、低減、復旧の手順を微調整することです。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
12.10.7 想定外の場所に保存された PAN が検出された場合に開始されるインシデント対応手順が用意されており、以下の内容が含まれる。 • カード会員データ環境（CDE）の外側で PAN が発見された場合の対処方法を決定する。これには、PAN の検索、安全な削除、および／または現在定義されているカード会員データ環境（CDE） への移行（該当する場合）などが含まれる。 • 機密性認証データが PAN と共に保存されているかどうかを特定する。 • アカウントデータの出所と、それがどのようにして想定外の場所に行き着いたかを特定する。 • アカウントデータが想定外の場所にある原因となったデータ漏えいまたはプロセスギャップを修正する。	**12.10.7.a** 文書化されたインシデント対応手順を調査し、想定外の場所で保存された PAN の検出への対応手順が存在し、開始できる状態にあり、この要件で指定されたすべての要素が含まれていることを確認する。	保存された PAN が想定外の場所で発見された場合に従うインシデント対応手順を文書化しておくことで、必要な是正措置を特定し、将来の漏洩を防止することができます。
カスタマイズアプローチの目的	**12.10.7.b** 担当者にインタビューし、対応措置の記録を調査して、想定外の場所に保存された PAN が検出された場合に、インシデント対応手順が実行されることを確認する。	**グッドプラクティス**
想定外の場所で平文 PAN が検出された場合、迅速に対応、分析、対処するためのプロセスが整備されている。		カード会員データ環境（CDE）の外側で PAN が発見された場合、1）他のデータとは別に保存されたのか、それとも機密性認証データとともに保存されたのかを判断し、2）データの出所を特定し、3）カード会員データ環境（CDE） の外側にデータがある原因となったコントロールギャップを特定するための分析を行う必要があります。 事業体は、PAN が予期せぬ場所に保存される原因となった、ビジネスプロセス、ユーザの行動、不適切なシステム設定などの要因があるかどうかを検討する必要があります。そのような寄与要因がある場合は、本要件に従って再発防止のための対処を行うべきです。

要件とテスト手順		ガイダンス
適用に関する注意事項 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に考慮する必要がある。*		

付録A　　追加の PCI DSS 要件

この付録は異なる事業体の種類に対する追加の PCI DSS 要件が含まれています。この付録のセクションには以下が含まれています：

- 付録 A1:　　マルチテナントサービスプロバイダ向けの PCI DSS 追加要件
- 付録 A2:　　カード提示 POS POI 端末接続用に SSL / 初期の TLS を使用する事業体向けの PCI DSS 追加要件
- 付録 A3:　　指定事業体向け追加検証(DESV)

各項目にはガイダンスと適用情報が記載されています。

付録 A1: マルチテナントサービスプロバイダ向けの PCI DSS 追加要件

セクション	
A1.1	マルチテナントサービスプロバイダは、すべての顧客環境およびデータを保護し、分離する。
A1.2	マルチテナントサービスプロバイダは、すべての顧客に対して、ロギングとインシデントレスポンスを容易にする。

概要

すべてのサービスプロバイダは、顧客に提供するサービスに適用される、自身の環境に対する PCI DSS 要件を満たす責任を負います。さらに、マルチテナントサービスプロバイダは、本付録の要件を満たす必要があります。

マルチテナントサービスプロバイダーは、システムリソース（物理サーバーや仮想サーバーなど）、インフラ、アプリケーション（SaaS を含む）、データベースなどを共有し、加盟店や他のサービスプロバイダーに対してさまざまな共有サービスを提供するサードパーティサービスプロバイダーの一種である。サービスには、単一の共有サーバー上での複数のエンティティのホスティング、電子商取引および/または「ショッピングカート」サービスの提供、Web ベースのホスティングサービス、支払いアプリケーション、様々なクラウドアプリケーションおよびサービス、支払いゲートウェイおよびプロセッサへの接続が含まれますが、これらに限定されるものではありません。

機器、スペース、帯域幅がレンタルベースで利用可能な、共有データセンターサービスのみを提供するサービスプロバイダ（しばしばコロケーションまたは「コロ」プロバイダと呼ばれます）は、本付録の目的上、マルチテナントサービスプロバイダとはみなされません。

注：マルチテナントサービスプロバイダがこれらの要件を満たしていても、各顧客はその環境に適用される PCI DSS 要件に準拠し、該当する場合は準拠を確認する責任を負います。多くの場合、プロバイダと顧客の間で（おそらく環境の異なる側面について）責任を共有する PCI DSS 要件があります。要件 12.8 および 12.9 は、すべてのサードパーティサービスプロバイダ（TPSP）とその顧客の関係、および両者の責任に固有の要件を定義しています。これには、顧客が受けている特定のサービスの定義、それに加えてどの PCI DSS 要件を満たすことが顧客の責任であるか、どれが TPSP の責任であるか、どの要件が顧客と TPSP の両方で共有されるかが含まれます。

要件とテスト手順		ガイダンス
A1.1 マルチテナントのサービスプロバイダは、すべての顧客の環境とデータを保護し、分離しています。		
定義されたアプローチの要件 **A1.1.1** 論理的分離は次のように実装されている。 • プロバイダは、承認なしに顧客の環境にアクセスすることはできない。 • 顧客は承認なしにプロバイダの環境にアクセスできない。 **カスタマイズアプローチの目的** 顧客はプロバイダの環境にアクセスできない。プロバイダは、顧客の環境に承認なしにアクセスできない。 **適用に関する注意事項** *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に考慮する必要がある。*	**定義されたアプローチのテスト手順** **A1.1.1** 文書、システムおよびネットワーク構成を調査し、担当者にインタビューして、この要件で指定されているすべての要素に従って論理的分離が実装されていることを確認する。	**目的** プロバイダの環境と顧客の環境との間に制御がなければ、プロバイダの環境内の悪意のある者が顧客の環境を侵害する可能性があり、同様に、顧客の環境内の悪意のある者がプロバイダとプロバイダの他の顧客を侵害する可能性もあります。 マルチテナント環境は、互いに隔離され、プロバイダのインフラストラクチャからも隔離され、両者間の接続がない状態で個別に管理できるようにする必要があります。 **グッドプラクティス** プロバイダは、顧客からのアクセスを想定した環境（例えば、設定や課金のポータルサイト）と、プロバイダの権限を持つ担当者のみがアクセスできるプロバイダのプライベート環境との間に、強力な分離を確保すべきです。 サービスプロバイダによる顧客環境へのアクセスは、要件 8.2.3 に従って実行されます。 **その他の情報** *情報補足：*クラウド環境に関する詳しいガイダンスは、*PCI SSC クラウドコンピューティングガイドライン*を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **A1.1.2** 各顧客が、自身のカード会員データおよび カード会員データ環境（CDE） にアクセスする権限のみを有するように、制御が実施される。	**定義されたアプローチのテスト手順** **A1.1.2.a** 文書を調査し、各顧客が自身のカード会員データおよびカード会員データ環境（CDE） にアクセスする権限のみを持つようなコントロールが定義されていることを確認する。 **A1.1.2.b** システム構成を調査し、顧客が自身のアカウントデータとカード会員データ環境（CDE）にのみアクセスする特権を確立していることを確認する。	**目的** マルチテナントサービスプロバイダは、各顧客が自身の環境とカード会員データ環境（CDE）にのみアクセスできるようにコントロールを定義し、ある顧客の環境から別の顧客の環境への未承認のアクセスを防止することが重要です。 **例** IaaS のようなクラウドベースのインフラストラクチャでは、顧客のカード会員データ環境（CDE）は、オペレーティングシステム、ファイル、メモリなど、顧客によって構成され管理される仮想ネットワークデバイスや仮想サーバを含む場合があります。
カスタマイズアプローチの目的 顧客は他の顧客の環境にアクセスできない。		
定義されたアプローチの要件 **A1.1.3** 各顧客が自身に割り当てられたリソースにのみアクセスできるようなコントロールが実施されている。	**定義されたアプローチのテスト手順** **A1.1.3** 顧客の特権を調査し、各顧客が自身に割り当てられたリソースにしかアクセスできないことを確認する。	**目的** 他の顧客の環境やアカウントデータへの不用意な、あるいは意図的な影響を防ぐため、顧客ごとに割り当てられたリソースのみにアクセスできるようにすることが重要です。
カスタマイズアプローチの目的 顧客は、他の顧客に割り当てられたリソースに影響を与えることができない。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件 **A1.1.4** 顧客環境を分離するための論理的分離コントロールの有効性を、少なくとも半年に一度、ペネトレーションテストにより確認している。 **カスタマイズアプローチの目的** 顧客の環境と他の環境とのセグメンテーションが有効であることを定期的に確認している。 **適用に関する注意事項** マルチテナントサービスプロバイダ環境における顧客間の適切な分離のテストは、要件 11.4.6 で規定されているペネトレーションテストに追加される。 この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に *考慮* する必要がある。	**定義されたアプローチのテスト手順** **A1.1.4** 直近のペネトレーションテストの結果を調べ、テストにより顧客環境の分離に使用される論理的分離コントロールの有効性が確認されたことを確認する。	**目的** マルチテナントサービスプロバイダは、顧客間のセグメンテーションを管理する責任があります。 セグメンテーションの管理が有効であることを技術的に保証しなければ、サービスプロバイダの技術の変更により、サービスプロバイダの全ての顧客にわたって悪用されうる脆弱性が不注意に生じる可能性があります。 **グッドプラクティス** 分離技術の有効性は、サービスプロバイダが作成した顧客環境を模した仮設環境（モックアップ）を用いて、1）仮設環境から別の環境へアクセスする、2）インターネットから仮設環境へアクセスする、を試みることによって確認することができます。

要件とテスト手順		ガイダンス
A1.2 マルチテナントサービスプロバイダは、すべての顧客のログ記録とインシデント対応を促進する。		
定義されたアプローチの要件 **A1.2.1** 監査ログ機能が各顧客の環境に対して有効化されており、以下を含む PCI DSS 要件 10 と一致する。 • ログは、一般的なサードパーティのアプリケーションに対して有効になっている。 • ログはデフォルトで有効になっている。 • ログは、所有する顧客のみが確認できるようになっている。 • ログの保管場所が所有する顧客に明確に伝えられている。 • ログのデータおよび可用性は、PCI DSS 要件 10 と一致している。 **カスタマイズアプローチの目的** 他の顧客の機密保持に影響を与えることなく、すべての顧客がログ機能を利用できる。	**定義されたアプローチのテスト手順** **A1.2.1** 文書およびシステム構成設定を調査し、プロバイダがこの要件で指定されたすべての要素に従って、各顧客環境の監査ログ機能を有効にしていることを確認する。	**目的** ログ情報は、セキュリティインシデントの検出とトラブルシューティングに有用であり、フォレンジック調査にとって非常に貴重です。したがって、顧客はこれらのログにアクセスする必要があります。しかし、ログ情報は攻撃者が偵察のために使用することもできるため、顧客のログ情報には、そのログに関連する顧客のみがアクセスできるようにしなければなりません。
定義されたアプローチの要件 **A1.2.2** 顧客のセキュリティインシデントが疑われる、または確認された場合に、迅速なフォレンジック調査を支援および／または促進するプロセスまたは仕組みが導入される。	**定義されたアプローチのテスト手順** **A1.2.2** 文書化された手順を調査し、プロバイダが、顧客のセキュリティインシデントが疑われる場合または確認された場合に、関連するサーバの迅速なフォレンジック調査を支援および／または促進するプロセスまたは仕組みを有していることを確認する。	**目的** カード会員データの機密保持違反が疑われる、または確認された場合、顧客のフォレンジック調査官は、侵害の原因を突き止め、攻撃者を環境から排除し、すべての不正アクセスを確実に除外することを目的としています。 *(次ページに続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 セキュリティインシデントが疑われる場合、または確認された場合、すべての顧客がフォレンジック調査を容易に利用できる。		フォレンジック調査官の要求に迅速かつ効率的に対応することで、調査官が顧客の環境を保護するためにかかる時間を大幅に短縮することができます。
定義されたアプローチの要件 **A1.2.3** 疑われる、または確認されたセキュリティインシデントや脆弱性を報告し、対処するためのプロセスまたはメカニズムが実装されている。 • 顧客がセキュリティインシデントや脆弱性をプロバイダに安全に報告できる。 • プロバイダは、要件 6.3.1 に従って、疑いまたは確認されたセキュリティインシデントや脆弱性に対処し改善する。	**定義されたアプローチのテスト手順** **A1.2.3** 文書化された手順を調査し、担当者にインタビューして、プロバイダがこの要件で指定されたすべての要素に従って、疑いまたは確認されたセキュリティインシデントおよび脆弱性を報告し、対処するためのメカニズムを持っていることを確認する。	**目的** 提供するサービスのセキュリティ脆弱性は、サービスプロバイダの全ての顧客のセキュリティに影響を与える可能性があるため、サービスプロバイダが確立したプロセスに従って管理し、侵害の可能性が最も高い脆弱性を優先的に解決する必要があります。 顧客は、サービスを利用しているなかで、脆弱性やセキュリティの設定ミスに気付く可能性が考えられます。 顧客がセキュリティインシデントや脆弱性を報告するための安全な方法を導入することは、顧客が潜在的な問題を報告することを促し、プロバイダが環境内の潜在的な問題について迅速に知り、対処することを可能にします。
カスタマイズアプローチの目的 セキュリティインシデントや脆弱性の疑いがある、または確認された場合、発見され、対処される。適切な場合には顧客に通知される。		
適用に関する注意事項 *この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に考慮する必要がある。*		

付録 A2: カード提示 POS POI 端末接続用に SSL / 初期の TLS を使用する事業体向けの PCI DSS 追加要件

セクション
A2.1 SSL や初期の TLS を使用している POI 端末は、既知の SSL/TLS 脆弱性を突いた攻撃の影響を受けることはありません。

概要

本付録は、POS POI 端末への接続を提供するサービスプロバイダを含め、POS POI 端末を保護するためのセキュリティ制御として SSL/初期の TLS を使用する事業体にのみ適用されます。

POS POI 端末の接続に SSL および初期の TLS を使用している事業者は、できるだけ早く強力な暗号プロトコルにアップグレードするよう努力しなければなりません。また、SSL や初期の TLS がまだ存在しない環境に導入してはいけません。本書の発行時点では、既知の脆弱性を POS POI 決済端末で悪用することは困難です。しかし、新しい脆弱性はいつでも出現する可能性があり、脆弱性の動向を常に把握し、既知の脆弱性の影響を受けやすいかどうかを判断するのは組織の責任です。

直接影響を受ける PCI DSS の要件は以下の通りです。

- **要件 2.2.5：**安全でないサービス、プロトコル、またはデーモンが存在する場合、ビジネス上の正当性を文書化し、安全でないサービス、プロトコル、またはデーモンを使用するリスクを低減する追加のセキュリティ機能を文書化し、実装する。
- **要件 2.2.7：**コンソール以外の管理者アクセスはすべて強力な暗号を使用して暗号化されている。
- **要件 4.2.1：**強力な暗号とセキュリティプロトコルを実装し、オープンな公共ネットワークでの伝送時に PAN を保護する。

この付録に詳述されているように、POS POI 端末接続の場合を除き、これらの要件を満たすためのセキュリティ制御として SSL および初期の TLS を使用してはいけません。POS POI 端末の SSL／初期の TLS からの移行に取り組む事業体を支援するために、以下の規定が含まれます。

- 新規に実装する POS POI 端末は、セキュリティ制御として SSL または初期の TLS を使用してはならない。
- すべての POS POI 端末のサービス提供者は、安全なサービスを提供しなければならない。
- SSL および／または初期の TLS を使用する既存の POS POI 端末の実装をサポートするサービスプロバイダは、正式なリスク低減策および移行計画を策定する必要がある。
- カード提示環境における POS POI 端末で、SSL および初期の TLS に関する既知の脆弱性がないことが確認された **SSL/TLS の接続終端地点**は、セキュリティ制御として SSL/初期の TLS の使用を継続することができる。

本付録の要件は、カスタマイズアプローチの対象外です。

要件とテスト手順		ガイダンス
A2.1 SSL および／または初期の TLS を使用する POI 端末は、既知の SSL/TLS 脆弱性を突いた攻撃の影響を受けないこと。		
定義されたアプローチの要件 **A2.1.1** 加盟店または決済受付場所の POS POI 端末が SSL および／または初期の TLS を使用する場合、事業体は、そのデバイスがこれらのプロトコルに対する既知の脆弱性を突いた攻撃の影響を受けないことを確認する。 **カスタマイズアプローチの目的** この要件は、カスタマイズアプローチの対象外である。 **適用に関する注意事項** この要件は、加盟店などの POS POI 端末を有する事業者に適用されることを意図している。この要件は、POS POI 端末の終端箇所または接続先として機能するサービスプロバイダを対象としていない。要件 A2.1.2 および A2.1.3 は、POS POI サービスプロバイダに適用される。 現在、脆弱性を突いた攻撃を受けにくい POS POI 端末の許容範囲は、現在知られているリスクに基づいている。POS POI 端末が影響を受けやすい新しい脆弱性を突いた攻撃が登場した場合、POS POI 端末を直ちに更新する必要がある。	**定義されたアプローチのテスト手順** **A2.1.1** SSL および／または初期の TLS を使用する POS POI 端末について、事業体が、SSL/初期の TLS に関する既知の脆弱性を突いた攻撃の影響を受けないことを確認する文書（たとえば、ベンダの文書、システム／ネットワーク構成の詳細）を持っていることを確認する。	**目的** カードを提示する環境で使用される POS POI 端末は、現在の既知の攻撃手法に対して耐性があることを示すことができる場合、SSL/初期の TLS の使用を継続することができます。 **グッドプラクティス** しかし、SSL は古い技術であり、将来的にさらなるセキュリティ脆弱性の影響を受ける可能性があるため、POS POI 端末はできるだけ早く安全なプロトコルにアップグレードすることを強く推奨します。SSL/初期の TLS が不要な環境では、これらのバージョンの使用とフォールバックを無効化する必要があります。 **その他の情報** 詳細なガイダンスについては、最新の SSL/初期の TLS に関する PCI SSC 情報補足を参照してください。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** アクワイアラまたはアクワイアラプロセッサなどのサービスプロバイダを含むがこれに限定されない POS POI 終端箇所は、サービスプロバイダが、サービスプロバイダ環境のためにこれらの接続をサポートするリスクを軽減するコントロールを行っていることを示すことができる場合、SSL/初期の TLS を継続して使用することができます。 **グッドプラクティス** サービスプロバイダは、SSL/初期の TLS を使用しているすべての顧客に対し、その使用に伴うリスクと安全なプロトコルへの移行の必要性を伝えるべきです。 **定義** リスク軽減と移行計画とは、安全なプロトコルへの移行計画を詳述し、移行が完了するまでの間、SSL/初期の TLS に関連するリスクを軽減するために事業者が実施するコントロールを記述した、事業者が作成する文書です。 **その他の情報** リスク軽減および移行計画に関する詳細なガイダンスについては、最新の SSL/初期の TLS に関する PCI SSC 情報補足を参照してください。
A2.1.2 ***サービスプロバイダのみ追加要求：*** A2.1 に定義された SSL および／または初期の TLS を使用する POS POI 端末への既存の接続ポイントを持つすべてのサービスプロバイダは、以下を含む正式なリスク軽減および移行計画を策定している。 • どのようなデータが伝送されるか、SSL/初期の TLS を使用および／またはサポートするシステムの種類と数、および環境の種類を含む使用状況の説明 • リスクアセスメントの結果およびリスク低減策 • SSL/初期の TLS に関連する新しい脆弱性を監視するプロセスの説明 • SSL/初期の TLS が新規環境に実装されないことを確実にする為に実施された変更管理プロセスの記述 • 将来的に SSL/初期の TLS を置き換える為の、移行プロジェクト計画の概要	**A2.1.2** ***サービスプロバイダ評価のみの追加テスト手順：*** 文書化されたリスク軽減および移行計画をレビューし、この要件で指定されたすべての要素が含まれていることを確認する。	
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
適用に関する注意事項 この要件は、評価対象の事業者がサービスプロバイダである場合にのみ適用される。		
定義されたアプローチの要件 **A2.1.3 サービスプロバイダのみ追加要求：**すべてのサービスプロバイダは、安全なサービスを提供する。	**定義されたアプローチのテスト手順** ***A2.1.3 サービスプロバイダ評価のみの追加テスト手順：***サービスプロバイダがそのサービスのために安全なプロトコルオプションを提供していることを確認するために、システム構成とサポートドキュメントを調査する。	**目的** 顧客が、SSL や初期の TLS を使用する際の脆弱性を排除するために、POI をアップグレードすることを選択できるようにする必要があります。多くの場合、顧客は POS POI 資産を安全でないプロトコルから安全なプロトコルに移行するために段階的または漸進的なアプローチを取る必要があるため、サービスプロバイダが安全なサービスをサポートすることが必要になります。 **その他の情報** 詳細なガイダンスについては、最新の SSL/初期の TLS に関する PCI SSC 情報補足を参照してください。
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外である。		
適用に関する注意事項 この要件は、評価対象の事業者がサービスプロバイダである場合にのみ適用される。		

付録 A3: 指定事業体向け追加検証(DESV)

セクション
A3.1 PCI DSS 準拠のプログラムが実施されている。
A3.2 PCI DSS の適用範囲が文書化され、確認されている。
A3.3 PCI DSS が日常業務（BAU）の活動に組み込まれている。
A3.4 カード会員データ環境への論理的なアクセスが制御および管理されている。
A3.5 疑わしいイベントを特定し、対処している。

概要

この付録は、既存の PCI DSS 要件の追加確認が必要であるとペイメントブランドまたはアクワイアラによって指定された事業体にのみ適用されます。事業体は、アクワイアラまたはペイメントブランドによって指示された場合に限り、この付録に従って評価を受ける必要があります。この付録が適用される可能性のある事業体の例には、以下が含まれます。

- 大量のアカウントデータを保存、処理、および／または伝送している。
- アカウントデータの集約場所を提供している、または
- アカウントデータの重大な、または度重なる侵害を受けたことがある。

さらに、他の PCI 基準がこの付録の完了を参照することがあります。

*これらの補助的な検証ステップは、日常業務（BAU）プロセスの検証および強化された検証と評価範囲の考察を通じて、PCI DSS コントロールが効果的かつ継続的に維持されていることのさらなる保証を提供することを目的としています。**注：**一部の要件は、特定の活動が実施されるための時間枠（例えば、3 カ月に 1 回以上、6 カ月に 1 回以上）を定義しています。評価担当者が以下を検証する場合、この文書の初回の評価では、前年 1 年間に、前記の時間枠すべてにおいて活動が実施されることは求められません：。*

適用される要件に従って直近の時間枠（例えば、直近の 3 カ月間または 6 カ月間）で実施されている。および

- *事業体が定義された時間枠内で活動の実施を継続するポリシーおよび手順を文書化している*

初回の評価後、その後の年度において、要求される各期間内に活動が実施されていなければいけません（例えば、3 カ月ごとに必要な活動は、90 日を超えない間隔で前年度に少なくとも 4 回実施されていなければならない）。

PCI DSS のすべての要件が、PCI DSS の評価を受ける可能性のあるすべての事業体に適用されるわけではありません。このため、一部の PCI DSS 要件が当該付録で重複しています。本付録に関するご質問は、アクワイアラまたはペイメントブランドにお問い合わせください。

要件とテスト手順		ガイダンス
A3.1 PCI DSS 準拠プログラムが実施されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
A3.1.1 アカウントデータの保護と、以下を含む PCI DSS 準拠プログラムについて、経営陣が責任を持つこと。 • PCI DSS 準拠の維持に関するすべての責任 • PCI DSS 準拠プログラムの憲章の定義 • 少なくとも 12 か月に 1 回、PCI DSS 準拠の取り組みや改善活動を含む課題について経営層および取締役会へ最新情報を提供する。 **PCI DSS 参照**:*要件 12*	**A3.1.1.a** 文書を調べ、経営層が事業体の PCI DSS 準拠の維持に関するすべての責任を割り当てていることを確認する。	**目的** 経営層への PCI DSS 準拠の責任の割り当ては、経営レベルにおける PCI DSS 準拠プログラムの可視性を確実にし、プログラムの有効性と戦略的優先事項への影響を判断するための適切な質問の機会を与えます。 **グッドプラクティス** 経営幹部には、経営幹部の役職、取締役会、またはそれに相当する役職が含まれる場合がある。具体的な肩書きは、特定の組織構造によって異なります。 PCI DSS 準拠プログラムに対する責任は、個々の役割または組織内の事業単位に割り当てることができます。
	A3.1.1.b 会社の PCI DSS 憲章を調べて、PCI DSS 準拠プログラムを構成する条件を概説していることを確認する。	
カスタマイズアプローチの目的	**A3.1.1.c** 経営層と取締役会の議事録や議案を調べ、PCI DSS 準拠の取り組みや改善活動が、少なくとも 12 か月に 1 回コミュニケーションされていることを確認する。	
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
A3.1.2 正式な PCI DSS 準拠プログラムには以下を含める： • 日常業務（BAU）を含む PCI DSS 準拠全体を維持および監視するための活動を定義する。 • 年次の PCI DSS 評価プロセス • PCI DSS 要件の継続的な検証プロセス（たとえば、毎日、毎週、3 カ月ごとなど、要件ごとに該当する場合） • 戦略的なビジネス上の意思決定に対する PCI DSS の潜在的な影響を判断するためのビジネス影響分析を実行するためのプロセス **PCI DSS 参照**: *要件 1～12*	**A3.1.2.a** 情報セキュリティポリシーと手順を調べて、この要件で指定されているすべての要素を含む正式な PCI DSS 準拠プログラムのプロセスが定義されていることを確認する。 **A3.1.2.b** 担当者にインタビューし、準拠活動を観察して、この要件で指定されたすべての要素に従って正式な PCI DSS 準拠プログラムが実施されていることを確認する。	**目的** 正式な準拠プログラムは組織のセキュリティ対策の健全性を監視すること、制御の障害が発生した場合の積極的な対処、さらに組織全体の活動や準拠状態の効率的な共有を可能にします。 **グッドプラクティス** PCI DSS 準拠プログラムは、専用のプログラムであるか、包括的な準拠および／またはガバナンスプログラムの一部としてもよいですが、一貫性と効果的な評価を実証する明確に定義された方法論を含む必要があります。 PCI DSS の潜在的な影響を分析されるべき戦略的なビジネス上の決定には、合併と買収、新しい技術の購入、または新たな決済受付けチャネルが含まれます。 **定義** 組織全体の PCI DSS 準拠を維持および監視するには、日次、週次、月次、四半期ごと、または年に一回実施されるべき活動を特定し、これらの活動が適宜実行されていることを確認する（たとえば、セキュリティ自己評価または PDCA 手法を使用するなど）ことが含まれます。 **例** 準拠プログラムの管理を支援する方法論としては、PDCA（計画-実行-評価-改善）、ISO27001、COBIT、DMAIC、シックスシグマなどがあります。
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 具体的な PCI DSS 準拠の役割や責任の正式な定義は、継続中の PCI DSS 準拠の取り組みの説明責任や監視を確実にするために役立ちます。 **グッドプラクティス** オーナーシップは、リスクベースの意思決定を行う権限があり、特定の機能について説明責任がある個人に対して割り当てられる必要があります。職務は正式に定義されるべきであり、オーナーは自分の責任と説明責任について理解していることを実証できなければなりません。 準拠の役割は、1 人のオーナーに割り当てることも、異なる要件要素毎に複数のオーナーに割り当てることもできます。
A3.1.3 PCI DSS 準拠の役割と責任は、具体的に定義され、正式に一人以上の担当者が任命され、以下を含んでいること： • 日常業務（BAU）としての PCI DSS 管理 • 年次の PCI DSS 評価管理 • PCI DSS 要件の継続的な検証を管理する（たとえば、(日次、週次、四半期ごと等、要件ごとに該当する場合）。 • 戦略的なビジネス上の意思決定に対する PCI DSS の潜在的な影響を判断するビジネス影響分析の管理 **PCI DSS 参照**:*要件 12*	**A3.1.3.a** 情報セキュリティポリシーと手順を調査し、担当者にインタビューして、PCI DSS 準拠の役割と責任が明確に定義され、この要件のすべての要素に従って 1 人以上の担当者に正式に割り当てられていることを確認する。	
	A3.1.3.b 担当者にインタビューし、彼らが指定された PCI DSS 準拠の責任を熟知し、実施していることを確認する。	
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** PCI DSS 準拠の責任者は、その役割を果たすために、一般的なセキュリティ意識向上トレーニングで提供されるものを超える特定のトレーニングが必要です。 **グッドプラクティス** PCI DSS 準拠責任を負う個人は、個人が準拠責任を効果的に実施するために従うべき情報セキュリティに関する一般的な意識に加え、特定のセキュリティトピック、技術、プロセス、または方法論に焦点を当てた専門的なトレーニングを受講する必要があります。 トレーニングは、PCI SSC （PCI 意識向上、PCIP、ISA など）、ペイメントブランド、アクワイアラ などの第三者が提供する場合もあれば、内部トレーニングの場合もあります。トレーニングの内容は、各自の職務に適用可能で、最新のセキュリティ脅威および／または PCI DSS のバージョンを含むものである必要があります。 **その他の情報** その他のガイダンスについては*セキュリティ教育プログラムを実施するためのベストプラクティス*を参照してください。
A3.1.4 PCI DSS 準拠責任を持つ担当者（A3.1.3 で識別される）に対して、少なくとも 12 カ月に 1 回、最新の PCI DSS および／または情報セキュリティトレーニングが提供される。 **PCI DSS 参照**:*要件 12*	**A3.1.4.a** 情報セキュリティポリシーおよび手順を調べて、PCI DSS および／または情報セキュリティトレーニングが、PCI DSS 準拠責任を持つ各役割に対して少なくとも 12 カ月に 1 回要求されていることを確認する。	
	A3.1.4.b 担当者にインタビューし、受講証明書またはその他の記録を調べて、PCI DSS 準拠責任を負う担当者が最新の PCI DSS および／または同様の情報セキュリティトレーニングを少なくとも 12 か月に 1 回受けていることを確認する。	
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
A3.2 PCI DSS の適用範囲が文書化され、検証されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	
A3.2.1 PCI DSS の適用範囲は、文書化され、少なくとも 3 カ月に 1 回、および適用範囲内の環境に大幅な変更があった場合に、正確性が確認される。最低でも、適用範囲の検証には以下が含まれる。 • さまざまな決済段階（オーソリゼーション、キャプチャ、決済、チャージバック、返金など）および受け入れチャネル（カード提示、カード非提示、電子商取引など）のすべてのデータフローを特定すること。 • 要件 1.2.4 に従って、すべてのデータフロー図を更新すること。 • 1）現在定義されているカード会員データ環境（CDE）以外の場所、2）カード会員データ（CHD）を処理するアプリケーション、3）システムとネットワーク間の伝送、4）ファイルのバックアップを含むがこれらに限定されない、アカウントデータが保存、処理、伝送される全ての場所を特定すること。 • 現在定義されているカード会員データ環境（CDE）の外部にあるアカウントデータについては、1）安全に削除する、2）現在定義されているカード会員データ環境（CDE）に移行する、3）現在定義されているカード会員データ環境（CDE）を拡張して含める、のいずれかを行う。	**A3.2.1.a** 文書化された適用範囲レビューのされた結果を調べ、担当者にインタビューすることで、レビューが以下のように実施されていることを確認する。 • 少なくとも四半期ごと • 適用範囲内の環境に大幅な変更があった場合 **A3.2.1.b**. 少なくとも四半期ごとに適用範囲レビューの文書化された結果を調べ、適用範囲の検証がこの要件で指定されたすべての要素を含んでいることを確認する。	**目的** PCI DSS 適用範囲の頻繁な確認は、PCI DSS 適用範囲が常に最新で、変化するビジネス目標に一致し、その結果、セキュリティ管理がすべての適切なシステムコンポーネントを保護することを保証するのに役立ちます。 **グッドプラクティス** 正確な適用範囲特定には、カード会員データ環境（CDE） および接続されているすべてのシステムコンポーネントを厳格に評価し、PCI DSS 要件に必要な適用範囲を決定することが含まれます。慎重な分析および継続的な監視を含むスコーピング活動は、適用範囲内のシステムが適切に保護されていることを確認するのに役立ちます。アカウントデータの場所を文書化する場合、事業体は以下の情報を含む表またはスプレッドシートの作成を検討することができます。 • データの保存場所（データベース、ファイル、クラウドなど）、保存目的、保存期間など • どのカード会員データ（CHD）要素が保存されているか（PAN、有効期限、カード会員名、および／またはオーソリゼーション完了前の機密認証データ（SAD）の要素） *(次頁に続く)*

要件とテスト手順		ガイダンス
• カード会員データ環境（CDE）内のすべてのシステムコンポーネント、カード会員データ環境（CDE）に接続されているもの、カード会員データ環境（CDE）のセキュリティ *(次頁に続く)* ィに影響を与える可能性のあるものを特定する。 • 使用中のすべてのセグメンテーションコントロールと、カード会員データ環境（CDE）がセグメンテーションされている環境（範囲外の環境の正当な理由を含む）を特定すること。 • カード会員データ環境（CDE）にアクセス可能なサードパーティ事業体へのすべての接続を特定すること。 • 識別されたすべてのデータフロー、アカウントデータ、システムコンポーネント、セグメンテーションコントロール、およびカード会員データ環境（CDE）にアクセスする第三者からの接続が範囲に含まれることを確認すること。 **PCI DSS 参照**:*PCI DSS 要件の範囲*、*要件 12.*		• データの保護方法（暗号化の種類と強度、ハッシュアルゴリズムと強度、トランケーション、トークン化） • 使用されているログの仕組み（エンタープライズソリューション、アプリケーションレベル、オペレーティングシステムレベルなど）の説明を含む、データストアへのアクセスのログの記録方法 内部システムおよびネットワークに加えて、ビジネスパートナー、リモートサポートサービスを提供する事業体、その他のサービスプロバイダなどの第三者機関からのすべての接続を特定し、PCI DSS の適用範囲に含めるかどうかを判断する必要があります。適用範囲の接続を特定したら、該当する PCI DSS コントロールを実装して、第三者からの接続が事業体の カード会員データ環境（CDE） を侵害するために使用されるリスクを低減することができます。 データ検出ツールまたは方法を使用して、PAN のすべてのソースと場所を容易に特定し、現在定義されている カード会員データ環境（CDE）の外部のシステムおよびネットワークに存在する PAN、または定義されているカード会員データ環境（CDE）内の予期しない場所（エラーログやメモリダンプファイルなど）に存在する PAN を検索することができます。このアプローチにより、これまで知られていなかった PAN の場所が検出

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外である。		され、PAN が排除されるか、適切に保護されることが保証されます。 **その他の情報** *情報補足：PCI DSS の適用範囲とネットワークセグメンテーション*を追加のガイダンスとして、参照してください。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.2.2 新システムの追加や新しいネットワーク接続を含め、システムまたはネットワークのすべての変更に対する PCI DSS 適用範囲への影響を判断する。プロセスには以下が含まれる。 • 正式な PCI DSS 影響評価を実施する。 • システムまたはネットワークに適用される PCI DSS 要件の識別 • 適切な PCI DSS 適用範囲の更新 • 影響評価の結果に対する責任者（A3.1.3 で定義された方法で）による文書化された署名 **PCI DSS 参照**:*PCI DSS 要件の適用範囲、要件 1～12*	**A3.2.2** システムまたはネットワークへの各変更について、PCI DSS 適用範囲への影響が決定され、この要件で指定されたすべての要素が含まれていることを確認するために、変更文書を調べ、担当者にインタビューする。	システムまたはネットワークの変更は、PCI DSS の適用範囲に大きな影響を与える可能性があります。たとえば、ネットワークセキュリティコントロールルールセットの変更により、ネットワークセグメント全体が適用範囲に含まれるようになったり、適切に保護する必要がある新しいシステムがカード会員データ環境（CDE）に追加されたりする場合があります。 変更に先立ち実施される正式な影響評価は、その変更がカード会員データ環境（CDE）のセキュリティに悪影響を与えないことを事業体に保証するものです。 *(次頁に続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的		**グッドプラクティス**
この要件は、カスタマイズアプローチの対象ではありません。		システムおよびネットワークの変更が事業体の PCI DSS 範囲に及ぼす潜在的な影響を判断するプロセスは、専用の PCI DSS 準拠プログラムの一部として実行することも、事業体の包括的な準拠プログラムおよび／またはガバナンスプログラムとして実行することもできます。
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.2.2.1 変更完了後、すべての新規または変更されたシステムおよびネットワークに関連するすべての PCI DSS 要件が実装されていることを確認し、該当する場合は文書を更新する。 **PCI DSS 参考資料**:*PCI DSS 要件の適用範囲、要件 1-12*	**A3.2.2.1** 変更履歴を調べ、担当者にインタビューし、影響を受けるシステム／ネットワークを観察し、関連するすべての PCI DSS 要件が実装され、変更箇所に応じて文書が更新されていることを確認する。	システムまたはネットワークに加えられたすべての変更を分析し、変更によって適用範囲に追加されたシステムまたは ネットワークに適切な PCI DSS コントロールがすべて適用されていることを確認するプロセスを持つことが重要です。 *(次頁に続く)*

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外です。		この確認を変更管理プロセスに組み込むことで、デバイスのインベントリおよび構成基準が最新化されること、必要に応じてセキュリティ管理が適用されるようにすることができます。 **グッドプラクティス** 変更管理プロセスには、PCI DSS 要件が実装されている証拠、または反復プロセスを通じて維持されていることを裏付ける証拠を含める必要があります。 **例** 確認すべき PCI DSS 要件は以下の通りですが、これらに限定されるものではありません。 • 変更を反映するためのネットワーク図の更新 • すべてのデフォルトパスワードを変更および不要なサービスの無効化を含め、システムが構成基準に従って構成されている • 必要な制御によりシステムが保護されている（ファイル整合性監視、マルウェア対策、パッチ、監査ログなど） *(次頁に続く)* • 機密性認証データを保存せず、すべてのアカウントデータ保存場所が文書化され、データ保存ポリシーと手順に組み込まれている • 新しいシステムは、四半期ごとの脆弱性スキャンプロセスに含まれる。

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 組織の構造とマネジメントは、効果的で安全な運用のための要件と規約を定義します。この構造の変更は、これまで PCI DSS コントロールを担当していた担当者の配置転換や削減または削除、引き継いだ新たな責任者がコントロールを確立できていないことなどにより、既存のコントロールおよびフレームワークにマイナスの影響を与える可能性があります。したがって、組織の構造および管理に変更があった場合は、PCI DSS の適用範囲およびコントロールを再検討して、コントロール実装され、有効であることを確認することが重要です。 **例** 組織構造の変更には、会社の合併や買収、セキュリティ管理の責任を負う担当者の大幅な変更または配置転換などが含まれるが、これらに限定されません。
A3.2.3 組織構造の変更により、PCI DSS の適用範囲およびコントロールの適用性への影響に関する正式な（内部）レビューが行われる。 **PCI DSS 参考資料**:*要件 12*	**A3.2.3** ポリシーと手順を調べて、組織構造の変更により、PCI DSS の適用範囲とコントロールの適用性に対する影響の正式な見直しが行われることを確認する。	
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外です。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** PCI DSS では通常、12 カ月ごとにペネトレーションテストによるセグメンテーションコントロールの確認を行うことが要求されています。 セグメンテーション制御の確認をより頻繁に行うことで、適用範囲外の信頼できないネットワークからカード会員データ環境（CDE）に横方向にピボットしようとする攻撃者に悪用される前に、セグメンテーションの障害を発見できる可能性があります。 **グッドプラクティス** 要件では、この範囲の確認は少なくとも 6 カ月に 1 回と大幅な変更の後に実施されると規定されていますが、カード会員データ環境（CDE）を他のネットワークから分離する効果を維持するために、この演習はできるだけ頻繁に実行されるべきです。 **その他の情報** *情報補足：ペネトレーションテストガイダンス*
A3.2.4 セグメンテーションを使用する場合、PCI DSS の適用範囲は以下のように確認される。 • 要件 11.4.1 で定義された事業体の方法論による。 • セグメンテーション制御に対して、少なくとも 6 カ月ごと、セグメンテーション制御／方法の変更後にペネトレーション入テストが実行される。 • ペネトレーションテストは、使用されているすべてのセグメンテーションコントロール／方法を対象とする。 • ペネトレーションテストは、セグメンテーションコントロール／方法が運用可能であり、効果的であること、およびカード会員データ環境（CDE）をすべての適用範囲外システムから分離することを確認する。 **PCI DSS 参考資料**:*要件 11*	**A3.2.4** 直近のペネトレーションテストの結果を調べ、テストがこの要件で指定されたすべての要素に従って実施されたことを確認する。	
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外です。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** PCI DSS では、適用範囲特定の一環として、被評価事業体はその環境内のすべての平文 PAN の存在を特定し、文書化することが要求されています。平文 PAN のすべてのソースと場所を特定し、現在定義されているカード会員データ環境（CDE）の外部のシステムとネットワーク、または定義されているカード会員データ環境（CDE）内の予期しない場所（エラーログやメモリダンプファイルなど）で平文 PAN を探すデータ発見方法を導入すると、平文 PAN のこれまで知られていなかった場所が検出されて適切にセキュリティが確保されるようになります。 **例** データ発見プロセスは、1）市販の入手可能なデータ発見ソフトウェア、2）自社開発のデータ発見プログラム、3）手動検索など、様々な方法で行うことができます。また、必要に応じ、複数の方法を組み合わせて使用することもできます。 使用する方法にかかわらず、取り組みの目的は平文 PAN のすべてのソースと場所（定義されたカード会員データ環境（CDE）内だけでなく）を見つけることです。
A3.2.5 以下のようなデータ発見方法が実施されている。 • PCI DSS の範囲を確認する。 • 少なくとも四半期ごと、カード会員データ環境（CDE）またはプロセスに大幅な変更があった場合に、平文 PAN のすべてのソースと場所を特定する。 • 現在定義されているカード会員データ環境（CDE）の外部のシステムおよびネットワークに存在する可能性のある平文 PAN に対処する。 **PCI DSS 参考資料**:*PCI DSS 要件の適用範囲*	**A3.2.5.a** 文書化されたデータ発見方法がこの要件で指定されたすべての要素を含んでいることを確認するために調査する。	
	A3.2.5.b 最近のデータ発見活動の結果を調べ、担当者にインタビューし、データ発見が少なくとも四半期ごと、およびカード会員環境やプロセスの大幅な変更後に実施されていることを確認する。	
カスタマイズアプローチの目的 この要件はカスタマイズされた手法の対象外です		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** データ発見のために使用される方法をテストするプロセスにより、アカウントデータ検出の完全性と正確性を保証します。 **グッドプラクティス** 完全性を期すため、適用範囲内のネットワークにあるシステムコンポーネントと適用範囲外のネットワークにあるシステムをデータ発見プロセスに含めるべきです。 データ発見プロセスは、使用されているすべてのオペレーティングシステムとプラットフォームで有効であるべきです。正確性のテストは、使用中のシステムコンポーネントやファイルフォーマットにテスト用 PAN を配置し、データ発見方法がテスト用 PAN を検出することを確認することで行うことができます。
A3.2.5.1 データ発見に使用される方法の確認は、以下のように行う。 • 手法の有効性が確認されている。 • 方法は、使用されているすべてのタイプのシステムコンポーネントおよびファイルフォーマット上の平文 PAN を発見することができる。 • データ発見方法の有効性が、少なくとも年に一回確認されている。 **PCI DSS 参考資料**:*PCI DSS 要件の適用範囲*	**A3.2.5.1.a** の場合 担当者にインタビューし、文書をレビューして確認する。 • 事業体は、データ発見に使用される手法の有効性をテストするプロセスを有している。 • このプロセスには、使用されているすべてのタイプのシステムコンポーネントおよびファイル形式において、その方法が平文 PAN を発見できることを確認することが含まれる。	
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外である。	**A3.2.5.1.b**. 有効性テストの結果を調べ、データ発見方法の有効性が少なくとも年に一回確認されていることを確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.2.5.2 カード会員データ環境（CDE）外で平文の PAN が検出された場合に開始される対応手順が実装されており、これには以下が含まれる。 • カード会員データ環境（CDE）外部で平文 PAN が発見された場合の対応（PAN の検索および修正、安全な削除、現在定義されているカード会員データ環境（CDE）への移行など）を決定する。 • データがどのようにしてカード会員データ環境（CDE）の外に出たかを識別する。 • カード会員データ環境（CDE）外へのデータ流出の原因となったデータリークまたはプロセスギャップを修正する。 • データのソースを特定する。 • トラックデータが PAN とともに保存されているかどうかを特定する。	**A3.2.5.2.a**. 文書化された対応手順を調べ、カード会員データ環境（CDE）外での平文 PAN の検出に対応する手順が定義され、この要件で指定されたすべての要素を含んでいることを確認する。 **A3.2.5.2.b** 担当者にインタビューし、対応活動の記録を調べることで、カード会員データ環境（CDE）の外側で平文 PAN が検出された場合に、改善策が実施されることを確認する。	カード会員データ環境（CDE）外で平文の PAN が検出された場合に従う対応手順を文書化しておくことで、必要な修正アクションを特定し、将来の漏洩を防止することができます。 **グッドプラクティス** カード会員データ環境（CDE）外で PAN が発見された場合、1）他のデータとは別に保存されたのか、それとも機密性認証データとともに保存されたのかを判断し、2）データの出所を識別し、3）データがカード会員データ環境（CDE）外にあることになったコントロールギャップを識別するための分析を実施する必要があります。 事業体は、ビジネスプロセス、ユーザの行動、不適切なシステム設定などの寄与要因により、PAN が予期せぬ場所に保存されたかどうかを検討する必要があります。そのような要因がある場合は、本要件に従って再発防止のための対処を行うべきです。
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外です。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 未承認の PAN がカード会員データ環境（CDE）から出ることを検知・防止するメカニズムを使用することで、組織はデータ損失につながる可能性がある状況を検知・防止することができます。 **グッドプラクティス** メカニズムがカバーする範囲は、電子メール、リムーバブルメディアへのダウンロード、プリンターへの出力などを含むが、これらに限定されません。 **例** 平文 PAN の不正な紛失を検知・防止するメカニズムには、データ損失防止（DLP）ソリューションなどの適切なツールの使用や、手動プロセスおよび手順が含まれる場合があります。
A3.2.6 平文 PAN が未承認の経路、方法、またはプロセスを経由してカード会員データ環境（CDE）から出ることを検知し、防止するためのメカニズムが実装されている。 • アクティブに動作している。 • 未承認の経路、メソッド、またはプロセスを介してカード会員データ環境（CDE）から出る平文の PAN を検出および防止するように構成されている。 • 未承認の経路、方法、またはプロセスを介してカード会員データ環境（CDE）から平文 PAN が流出したことを検出すると、監査ログとアラートを生成する。 **PCI DSS 参考資料**:*PCI DSS 要件の適用範囲、要件 12*	**A3.2.6.a** 文書を調べ、実装されたメカニズムを観察し、メカニズムがこの要件で指定されたすべての要素に準拠していることを確認する。	
	A3.2.6.b 監査ログとアラートを調査し、責任者にインタビューして、アラートが調査されていることを確認する。	
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.2.6.1 不正な経路、方法、またはプロセスを介して、平文 PAN をカード会員データ環境（CDE） から取り出そうとする試みを検知した際に開始される対応手順を実装する。対応手順は以下を含む必要がある。 • 責任者によって、警告をタイムリーに調査する手順 • データ流出を防ぐための、データ漏えいやプロセスギャップを必要に応じて改善する手順 **PCI DSS 参考資料**:*要件 12*	**A3.2.6.1.a** 文書化された対応手順を調べ、不正な経路、方法、またはプロセスを介してカード会員データ環境（CDE）から平文 PAN を取り出そうとした場合の対応手順が、この要件で指定されたすべての要素を含んでいることを確認する。 • 責任者によって、警告をタイムリーに調査する手順 • データ流出を防ぐための、データ漏えいやプロセスギャップを必要に応じて改善する手順	平文 PAN を不正な経路、方法、またはプロセスを介して取り出そうとする試みは、データを盗む悪意を示すか、あるいは適切な方法を知らない、または単に従わない正規の従業員の行動であるかもしれません。 これらの発生時にタイムリーな調査を行うと、修正を行う必要のある箇所を識別すること、および価値のある情報を提供することができ、脅威がどこからもたらされたかを理解するのに役立ちます。
カスタマイズアプローチの目的	**A3.2.6.1.b** 担当者にインタビューし、不正な経路や方法、またはプロセスを介して、平文 PAN がカード会員データ環境（CDE）からの送信を検知した際の対応記録を調べ、改善策が実施されたことを確認する。	
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
A3.3 通常業務（BAU）に PCI DSS を組み込んでいる。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 重要なセキュリティ制御の障害を迅速に（できるだけ早く）検出し、警告し、対処するための正式なプロセスがなければ、障害が検出されないまま、または長期間未解決のままになる可能性があります。さらに、時間的制約のある正式なプロセスがなければ、攻撃者はシステムを侵害し、カード会員データ環境（CDE）からアカウントデータを盗むのに十分な時間を持つことになります。 **グッドプラクティス** 具体的な障害の種類は、使用する機器システム部品の機能や技術によって異なる場合があります。典型的な障害は、システムがセキュリティ機能を果たさなくなること、またはファイアウォールがそのルールをすべて消去するかオフラインになるなど、意図した方法で機能しなくなることを含みます。
A3.3.1 重要なセキュリティ対策システムの障害のタイムリーな検出および報告のためのプロセスを実装する。重要なセキュリティ障害の例には以下を含むがこれらに限定されない： • ファイアウォール • IDS／IPS • ファイル整合性監視 • アンチウイルス • 物理的アクセス制御 • 論理的なアクセス制御 • 監査ログメカニズム • セグメンテーション制御（使用している場合） • 自動化された監査ログレビューの仕組み。*この箇条は発効日までのベストプラクティスである。詳細は下記の適用上の注意を参照すること。* • 自動化されたコードレビューツール（使用する場合）。 *この箇条は発効日までのベストプラクティスである。詳細は下記の適用上の注意を参照すること。* **PCI DSS 参考資料**:*要件 1～12* *(次ページに続く)*	**A3.3.1.a** 文書化されたポリシーと手順を調べ、この要件で指定されたすべての要素に従って、重要なセキュリティ対策システムの障害のタイムリーな検出および報告のためのプロセスが定義されていることを確認する。	

要件とテスト手順		ガイダンス
カスタマイズアプローチの目的 この要件は、カスタマイズアプローチの対象外。 **適用上の注意** *上記の箇条書き（自動ログレビュー機構および自動コードレビューツール（使用する場合））は、2025 年 3 月 31 日まではベストプラクティスである。2025 年 3 月 31 日以降は要件 A3.3.1 の一部として要求され、PCI DSS 評価中に十分に考慮する必要がある。*	**A3.3.1.b** 検出と警告のプロセスを調査し、担当者にインタビューして、この要件で指定されたすべての重要なセキュリティ制御についてプロセスが実装されていること、および重要なセキュリティ制御の各不具合によって警告が生成されることを確認する。	

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的** 重要なセキュリティ制御システムの障害による警告に迅速かつ効果的に対応しない場合、攻撃者はこの時間を利用して悪意のあるソフトウェアを挿入し、システムを制御したり、事業体環境からデータを盗んだりする可能性があります。 **グッドプラクティス** 文書化された証拠（例えば、問題管理システム内の記録）は、セキュリティ障害に対応するために実施されているプロセスや手順を裏付けるものであるべきです。さらに、担当者は、障害発生時の責任を認識していなければなりません。障害に対する措置および対応は、文書化された証拠に記録されるべきです。
A3.3.1.2 重要なセキュリティ対策の障害についてタイムリーに対応する。セキュリティ対策の障害に対応するためのプロセスには以下を含む： • セキュリティ機能を復旧させる。 • セキュリティ障害の発生期間（開始から終了までの日付と時間）を特定し、文書化する。 • 根本原因を含む障害原因の特定と文書化、および根本原因に対処するために必要な是正措置の文書化。 • 障害発生時に発生したセキュリティ上の問題を特定し、対処する。 • セキュリティ障害の結果、さらなる措置が必要かどうかを判断する。 • 障害原因の再発を防止するための管理策を実施する。 • セキュリティコントロールの監視を再開する。 **PCI DSS 参考資料**:*要件 1～12*	**A3.3.1.2.a** 文書化されたポリシーと手順を調査し、要員にインタビューして、この要件で指定されたすべての要素に 従ってセキュリティ管理の失敗に迅速に対応するプロセスが定義され実施されていることを検証します。	
	A3.3.1.2.b 記録を調査し、セキュリティ対策の障害が以下を含むように文書化されていることを確認する。 根本原因を含む失敗の原因の特定。 セキュリティ障害の期間（開始と終了の日時）。 • 根本原因に対処するために必要な是正措置の詳細。	
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.3.2 ハードウェアおよびソフトウェア技術は、少なくとも年に 1 回レビューし、それらが引き続き事業体の PCI DSS 要件を満たしているかどうかを確認する。 **PCI DSS 参考資料**:*要件 2、6、12.*	**A3.3.2.a** 文書化されたポリシーと手順を調べ、担当者にインタビューして、ハードウェアとソフトウェア技術をレビューして事業体の PCI DSS 要件を引き続き満たしているかどうかを確認するためのプロセスが定義され、実施されていることを確認する。	ハードウェアとソフトウェアの技術は常に進化しており、事業体は、使用する技術の変化と、それらの技術に対する脅威の進化を認識する必要があります。これらの技術について適切なレビューを行うことで、ベンダや開発者によって是正されないハードウェアやソフトウェアの脆弱性に備え、管理することができるようになります。
	A3.3.2.b ハードウェアおよびソフトウェア技術の最近のレビュー結果を確認し、レビューが少なくとも年に 1 回実施されていることを確認する。	**グッドプラクティス** また、ファームウェアのバージョンを確認し、ベンダによるサポートが最新であることを確認することも検討する必要があります。
カスタマイズアプローチの目的	**A3.3.2.c** 事業体の PCI DSS 要件を満たさないと判断されたテクノロジに対し、テクノロジを改善する計画が実施されていることを確認する。	また、事業体は、テクノロジベンダによる製品やプロセスの変更に注意し、そのような変更が事業体のテクノロジの使用にどのような影響を及ぼす可能性があるかを理解する必要があります。
この要件は、カスタマイズアプローチの対象外である。		PCI DSS の管理に影響を与える、または影響を及ぼすテクノロジを定期的にレビューすることで、購入、使用、および 導入の戦略を支援し、これらのテクノロジに依存する管理が引き続き有効であることを確認することができます。これらのレビューには、ベンダのサポートが終了したテクノロジや事業体のセキュリティニーズを満たせなくなったテクノロジのレビューが含まれますが、これらに限定されません。
適用上の注意		
このプロセスには、事業体の PCI DSS 要件を満たさなくなったテクノロジを改善する計画が含まれており、必要に応じてテクノロジの交換まで行うことができる。		

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.3.3 少なくとも四半期ごとに、日常業務の活動が守られていることを確認するレビューを実施する。レビューは、PCIDSS 準拠プログラム（A3.1.3 で定められた）で割り当てられた担当者によって実施され、以下を含む必要がある： • すべての日常業務（例、A3.2.2、A3.2.6、A3.3.1）について実施されていることの確認 • 要担当者がセキュリティポリシーと運用手順（例えば、日次のログレビュー、ファイアウォールのルールセットのレビュー、新規システムに対する構成基準など）に従っていることの確認 • すべての日常業務で対応済みと確認したことを含む、レビューが完了した方法の文書化。 • 年に一回の PCI DSS 評価で要求される文書化された証跡の収集。 • PCI DSS 準拠プログラム（A3.1.3 で定められた）のための責任を負った担当者による結果へのレビューと署名。 • すべての日常活動を対象とする、少なくとも 12 カ月の記録や文書の保存。 **PCI DSS 参考資料**:*要件 1～12*	**A3.3.3.a** ポリシーと手順を調べ、この要件で指定されたすべての要素に従って日常業務をレビューし、検証するためのプロセスが定義されていることを確認する。 **A3.3.3.b** 担当者にインタビューし、レビューの記録を調査して、以下を確認する。 • レビューが PCI DSS コンプライアンスプログラムに割り当てられた担当者によって実施されている。 • レビューが少なくとも 3 カ月に 1 回実施される。	セキュリティポリシーと手順が守られていることを定期的に確認することで、期待されるコントロールが有効であり、意図したとおりに機能しているという保証を得ることができます。これらのレビューの目的は、他の PCI DSS 要件を再実行することではなく、セキュリティ活動が継続的に実行されていることを確認することです。 **グッドプラクティス** これらのレビューは、適切な証拠が維持されていることを検証するためにも使用できます。たとえば、監査ログ、脆弱性スキャンレポート、ネットワークセキュリティ制御ルールセットのレビューなどは、事業体が次回の PCI DSS 評価に向けて準備する上で役に立ちます。 **例** 要件 1.2.7 を例にとると、要件 A3.3.3 は、少なくとも 3 カ月に 1 回、ネットワークセキュリティコントロールの設定のレビューが必要な頻度で行われていることを確認することで満たされている。一方、要件 1.2.7 は、要件で規定された構成のレビューを行うことで満たす。
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
A3.4 カード会員データ環境への論理的なアクセスが制御および管理されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.4.1 適用範囲内のシステムコンポーネントのユーザアカウントとアクセス権限を少なくとも 6 カ月ごとにレビューし、ユーザアカウントとアクセス権が職務に基づき適切であり、承認されていることを確認する。 **PCI DSS 参考資料**:*要件 7*	**A3.4.1** 責任者にインタビューし、サポートする文書を調べ、以下を確認する： • ユーザアカウントとアクセス権が、少なくとも 6 カ月ごとにレビューされている。 • アクセス権が職務に基づいた適切なものであり、すべてのアクセスが承認されていることをレビューにより確認している。	アクセス権の定期的な見直しは、ユーザの職責変更、システム機能の変更、その他の変更後に残存する過剰なアクセス権の発見に役立ちます。過剰なアクセス権を適切な時期に失効させないと、悪意のあるユーザに不正に利用される可能性があります。 この見直しは、（退職時に見逃していた）すべての退職されたユーザのアカウントが削除されていることを確認し、また、アクセスが不要になった第三者がアクセスを停止していることを確認するもう一つの機会を提供するものです。
カスタマイズアプローチの目的		
この要件は、カスタマイズアプローチの対象外である。		

要件とテスト手順		ガイダンス
A3.5 不審な事象が特定され、対応されている。		
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
A3.5.1 システム全体における攻撃パターンおよび望ましくない動作をタイムリーに特定する手法が実装されている。 • 異常や不審な行動が発生した場合に、それを識別すること。 • 疑わしい活動や異常が検出された場合、担当者に迅速に警告を発すること。 • 文書化された対応手順に従い、アラートに対応すること。 **PCI DSS 参考資料**: *必要条件 10, 12* を参照。	**A3.5.1.a** 文書をレビューし、担当者にインタビューすることで、システムに対する攻撃パターンと望ましくない行動をタイムリーに特定する、以下を含む方法論が定義され、実装されていることを確認する： • 異常や疑わしい活動が発生したことの特定 • 責任者へのタイムリーな警告の発行 • 文書化された対応手順に従った警告への対応	例えば、一元管理されたログ相関ツールや自動化されたログ相関ツールを使用して、システム全体の攻撃パターンや望ましくない動作を特定する能力は、データ侵害を防止、検出、またはその影響を最小化する上で重要です。すべての環境にログが存在することで、何か問題が発生したときに徹底的な追跡、警告、および分析が可能になります。ネットワークセキュリティ制御、IDS／IPS、ファイル整合性監視（FIM）システムなど、セキュリティ機能を実行する重要なシステムコンポーネントやシステムからの情報を裏付けるプロセスがなければ、侵害の原因を特定することは不可能ではないにしても、非常に困難となります。したがって、セキュリティ機能を実行するすべての重要なシステムコンポーネントとシステムのログを収集し、相関させ、維持する必要があります。これには、セキュリティ情報およびイベント管理（SIEM）、FIM、または変更検出などのリアルタイム分析、警告、および報告を提供するソフトウェア製品およびサービス手法の利用が含まれる可能性があります。
カスタマイズアプローチの目的	**A3.5.1.b** インシデント対応手順を調べ、担当者にインタビューし、以下を確認する。 • オンコール担当者が迅速にアラートを受信する。 • 警告は、文書化された対応手順に基づいて対応される。	
この要件は、カスタマイズアプローチの対象外である。		

付録B　代替コントロール

正当かつ文書化された技術上またはビジネス上の制約により、事業体が明示的に PCI DSS 要件を満たせない場合でも、他のコントロールまたは代替コントロールの実装により要件に関連するリスクを十分に軽減している場合は、代替コントロールを考慮することができます。

代替コントロールは、以下の基準を満たす必要があります。

1. 元の PCI DSS 要件の目的と厳格さを満たしていること。
2. 元の PCI DSS 要件で防御の対象とされているリスクを代替コントロールが十分に相殺するよう、元の PCI DSS 要件と同様のレベルの防御を提供する。要件の意図を理解するには、ほとんどの PCI DSS 要件のカスタマイズアプローチ*の目的*を参照してください。要件がカスタマイズアプローチの対象外で、カスタマイズアプローチの目的がない場合は、その要件のガイダンス欄の**目的**を参照してください。
3. その他の PCI DSS 要件「以上」のことを実現する。（単なるその他の PCI DSS 要件への準拠は代替コントロールになりません。）
4. 代替コントロールについてその他の要件「以上」であるかどうかを評価するときは、以下を考慮します。

注意： *すべての代替コントロールは、PCI DSS 評価を実施する評価者によってレビューされ、十分であることが検証される必要があります。代替コントロールの有効性は、コントロールが実装される環境の詳細、周囲のセキュリティコントロール、およびコントロールの構成に依存します。事業体は、特定の代替コントロールがすべての環境で有効であるとは限らないことを認識する必要があります。*

a. 既存の PCI DSS 要件が審査対象の項目に対してすでに要求されている場合は、代替コントロールと見なすことはできません。たとえば、コンソール以外の 管理アクセス用のパスワードは、平文の管理パスワードが傍受されるリスクを軽減するために暗号化して送信する必要があります。他のパスワード要件は平文パスワードの傍受リスクを軽減しないため、事業体は他の PCI DSS パスワード要件（侵入者のロックアウト、複雑なパスワードなど）を使用して暗号化パスワードの不足を補うことができません。また、その他のパスワード管理は、評価対象項目（パスワード）に対する PCI DSS 要件として既に存在しています。

b. 既存の PCI DSS 要件が別の領域で要求されているが、レビュー中の項目では要求されていない場合、それらを代替コントロールと見なすことは可能です。

c. 既存の PCI DSS 要件を新しいコントロールと組み合わせて、代替コントロールとすることができます。たとえば、ネットワークインターフェースを通じて悪用可能な脆弱性について、ベンダからセキュリティアップデートがまだ提供されていないため、事業体が対処できない場合、代替コントロールは、次のすべてを含むコントロールで構成される可能性があります。1) 内部ネットワークのセグメンテーション、2) 脆弱なインタフェースへのネットワークアクセスを必要なデバイスのみに制限する（IP アドレスまたは MAC アドレスのフィルタリング）、3) 脆弱なインタフェース宛のすべてのトラフィックを IDS／IPS で監視する。

5. PCI DSS 要件に準拠しないことによって生じる追加リスクに対処する。

6. 現在および将来の要件に対処する。過去に見落とされた要件（たとえば、2 四半期前にタスクの実行が要求されたが、そのタスクが実行されなかった場合など）には、代替コントロールで対応することはできない。

評価者は、各年次の PCI DSS 評価において代替コントロールを徹底的に評価し、各代替コントロールが、上記の 1 ～ 5 の項目に従って、元の PCI DSS 要件が対処するために設計されたリスクに適切に対処していることを確認する必要があります。

準拠を維持するには、評価完了後も代替コントロールが有効であることを確認するためのプロセスとコントロールを導入する必要があります。さらに、代替コントロールの結果は、評価に関する該当するレポート（ROC または SAQ など）の対応する PCI DSS 要件のセクションに文書化し、該当するレポートを要求元の事業体に提出する際に含める必要があります。

付録C　代替コントロールワークシート

事業体はこのワークシートを使用して、PCI DSS 要件を満たすために代替コントロールを使用するすべての要件について代替コントロールを定義する必要があります。代替コントロールは、対応する PCI DSS 要件のセクションの「ROC」の指示に従って文書化する必要があることにも注意してください。

***注：**:準拠を実現するために代替コントロールの使用を検討できるのは、正当な文書化された技術上またはビジネス上の制約がある事業体のみです。*

要件番号と定義：

	必要な情報	**説明**
1.　制約事項	当初の要件への準拠を妨げる、技術上またはビジネス上の正当な制約を文書化する。	
2.　代替コントロールの定義	代替コントロールを定義し、元のコントロールの目的および追加リスク（ある場合）にどのように対応するかを説明する。	
3.　目的	オリジナルのコントロールの目的（例えば、カスタマイズアプローチの目的）を定義する。	
	代替コントロールが満たす目的を特定する（注：これは、PCI DSS 要件のカスタマイズアプローチの目的である可能性もあるが、そうである必要はない）。	

4. 特定されるリスク	元のコントロールの不足によって生じる追加リスクをを特定する。	
5. 代替コントロールの有効性確認	代替コントロールがどのように検証され、テストされたかを定義する。	
6. 維持	代替コントロールを維持するためのプロセスおよびコントロールを定義する。	

付録D　カスタマイズアプローチ

このアプローチは、PCI DSS 要件のカスタマイズアプローチの目的を、定義された要件に厳密には従わない方法で満たすことを決定した事業体を対象としています。カスタマイズアプローチでは、事業体は要件のカスタマイズアプローチの目的を満たすために戦略的なアプローチを取ることができるため、その事業体に固有の方法で目的を満たすために必要なセキュリティコントロールを決定および設計することができます。

カスタマイズアプローチを実施する**事業体**は、以下の基準を満たす必要があります。

- カスタマイズされた各コントロールについて、付録 E1 のコントロールマトリクステンプレートに指定されているすべての情報を含む証拠を文書化し、維持する。
- 各カスタマイズされたコントロールについて、付録 E2 のターゲットリスク分析テンプレートに指定されているすべての情報を含むターゲットリスク分析（PCI DSS 要件 12.3.2） を実施し、文書化する。
- 有効性を証明するために各カスタマイズされたコントロールのテストを実施し、実施したテスト、使用した方法、テストした内容、テスト実施時期、およびテスト結果をコントロールマトリックスに文書化する。
- 各カスタマイズされたコントロールの有効性に関する証拠を監視し、維持すること。
- 完成したコントロールマトリックス、ターゲットリスク分析、テストの証拠、およびカスタマイズされたコントロールの有効性の証拠を評価者に提供する。

カスタマイズされたコントロールの評価を行う**評価者**は、以下の基準を満たす必要があります。

- カスタマイズされたコントロールを完全に理解し、事業体がカスタマイズアプローチの文書化および証拠の要件をすべて満たしていることを確認するために、事業体のコントロールマトリックス、ターゲットリスク分析、およびコントロールの有効性の証拠をレビューすること。
- 各カスタマイズされたコントロールの完全なテストを実施するために必要な適切なテスト手順を導き出し、文書化する。
- 各カスタマイズされたコントロールをテストし、事業体の実装が 1）要件のカスタマイズアプローチの目的を満たしているか、2）要件に対する「対応」の所見をもたらすかどうかを判断します。

- QSA は、常に QSA 資格要件で定義された独立性要件を維持します。これは、QSA がカスタマイズされたコントロールの設計または実施に関与する場合、その QSA は、そのカスタマイズされたコントロールのテスト手順の導出、評価、または評価の支援も行わないことを意味します。

事業体およびその評価者は、1）カスタマイズされたコントロールがカスタマイズアプローチの目的に完全に合致することに合意し、2）評価者がカスタマイズされたコントロールを完全に理解し、3）評価者が実施する導出テストを事業体が理解することを確認するために協力することが期待されます。

カスタマイズアプローチの使用は、QSA または ISA によって完了し、準拠に関する報告書（ROC）テンプレートの指示および PCI SSC ウェブサイトで利用可能な *PCI DSS v4.0 ROC テンプレートの使用に関する FAQ* の指示に従って文書化する必要があります。

SAQ（自己問診）に記入した事業者は、カスタマイズアプローチを使用することはできませんが、これらの事業者は、QSA または ISA に評価を実施させて ROC テンプレートに文書化することを選択することができます。

カスタマイズアプローチの使用は、コンプライアンスプログラムを管理する事業体（例えば、ペイメントブランドやアクワイアラ）によって規制される可能性があります。したがって、カスタマイズアプローチの使用に関する質問は、例えば、事業体が QSA を使用する必要があるか、カスタマイズアプローチを使用して評価を完了するために ISA を使用することができるかなど、これらの事業体に照会する必要があります。

注意： *カスタマイズアプローチでは、代替コントロールはオプションではありません。カスタマイズアプローチでは、事業体が要件であるカスタマイズアプローチの目的を満たすために必要なコントロールを決定し設計することができるため、事業体は、代替コントロールを実施する必要なく、その要件のために設計したコントロールを効果的に実施することが期待されています。*

付録E　カスタマイズアプローチをサポートするサンプルテンプレート

この付録には、カスタマイズアプローチの一部として事業体が文書化するための、コントロールマトリックスと標的リスク分析のテンプレートの例が含まれています。これらのテンプレートは、使用される可能性のあるフォーマットの例です。*事業体が本付録で提供される特定のフォーマットに従うことは要求されませんが、事業体のコントロールマトリックスおよび標的リスク分析には、これらのテンプレートで定義されるすべての情報を含める必要があります。*

E1 コントロールマトリックスのテンプレート例

以下は、事業体がカスタマイズされた実装を文書化するために使用することができるコントロールマトリックステンプレートのサンプルです。

付録D に記載されているように：*カスタマイズアプローチ*を使用する事業体は、コントロールマトリックスに記入し、実装された各コントロールの詳細（実装内容、コントロールが PCI DSS 要件の目的を満たすと事業体が判断した方法、コントロールが定義された要件を満たすことで達成されるのと少なくとも同等の保護レベルを提供する方法、コントロールの有効性について事業体が継続的に保証している方法）について説明する必要があります。

評価者は、各コントロールマトリックス内の情報を使用して、評価の計画および準備を行います。

このコントロールマトリックステンプレートのサンプルには、事業体が文書化し、カスタマイズされたバリデーションのために評価者に提供すべき最小限の情報が含まれています。この特定のテンプレートを使用する必要はありませんが、事業者のカスタマイズアプローチの文書には、このテンプレートで定義されたすべての情報が含まれており、事業者はこの正確な情報を評価者に提供することが要求されます。

コントロールマトリックスは、実施されたコントロールを検証するために、評価者が独自に適切なテスト手順を開発する必要性に取って代わるものではありません。 評価者は、コントロールが要件の目的を満たし、有効であり、適切に維持されていることを検証するために、必要なテストを実施しなければならないことに変わりはありません。また、コントロールマトリックスは、ROC テンプレートに規定されているカスタマイズされたバリデーションの報告要件に取って代わるものではありません。

コントロールマトリックスには、少なくとも以下の表の情報を含める必要がある。

カスタマイズされた方法で PCI DSS 要件を満たすためのコントロールマトリックス　テンプレートのサンプル 評価対象事業者が記入すること		
カスタマイズされたコントロールの名称／識別名	<このコントロールをどのように参照したいかを事業者が定義する>。	
PCI DSS 要件の番号とこのコントロールで満たされる目的	要件番号: 要件番号:	目的: 目的:
コントロールの詳細		
実装されているコントロール（複数可）は**何**ですか？	<コントロールが何であり、何をするのかを記述する事業体>。	
コントロールは**どこ**で実施されていますか？	<コントロールを実施・管理する施設やシステムの構成要素の位置を特定する事業体＞。	
いつ制御を行うのですか？	<例えば、リアルタイムで連続的に実行されるか、NN 時に XX 間隔で実行されるようスケジュールされているかなどです。＞	
コントロール（複数可）に対する全体的な責任と説明責任を持つのは**誰**ですか？	<事業体には、この管理に対する責任とアカウンタビリティを持つ個々の担当者／役割の詳細が含まれています>。	
コントロールの管理、維持、監視に関与しているのは**誰**ですか？	<事業体は、該当する場合、コントロールを管理、維持、監視する個々の担当者／役割、および／またはチームの詳細を含みます>。	

カスタマイズされた方法で PCI DSS 要件を満たすためのコントロールマトリックス　テンプレートのサンプル 評価対象事業者が記入すること	
コントロール（複数可）が使用されている各 PCI DSS 要件について、事業体は以下の詳細を提供します。	
事業体は、実装されたコントロールが、PCI DSS 要件の***カスタマイズアプローチ***（***目的***）をどのように満たすかを説明します。	<事業体は、コントロールが PCI DSS 要件のカスタマイズアプローチの目的をどのように満たしているかを説明し、関連する結果を要約します。>
事業体は、コントロールが該当する要件の目的に適合していることを**実証するテスト**およびそのテストの結果を記述します。	<事業体は、コントロールが PCI DSS 要件の目的を満たしていることを証明するために実施したテストを説明し、関連する結果をまとめます。>
事業者は、実施した個別のターゲットリスク分析の結果を簡潔に説明し、**実施した制御**を説明し、その結果、制御が該当する PCI DSS 要件の定義されたアプローチと少なくとも同等のレベルの保護を提供することをどのように検証するかを説明します。*このリスク分析を文書化する方法の詳細については、別の「ターゲットリスク分析テンプレート」を参照してください。*	<ターゲットリスク分析で別途詳述されているこのコントロールのリスク分析結果を簡潔に説明します>。
事業体は、コントロール（複数可）を維持し、その有効性を継続的に保証するために**実施した対策**を記述する。*例えば、統制の有効性をどのように監視しているか、統制の失敗をどのように発見し対処しているか、また、取られた措置などです。*	<事業体は、統制がどのように維持され、統制の有効性がどのように保証されているかを記述しています>。

E2 ターゲットリスク分析テンプレート例

以下は、事業体がカスタマイズした実施に使用できるターゲットリスク分析テンプレートのサンプルです。*事業体がこの特定の書式に従うことは要求されていませんが、カスタマイズアプローチの文書には、このテンプレートで定義されたすべての情報が含まれている必要があります*。

付録 D に記載されているように：*カスタマイズアプローチ*を使用する事業体は、PCI DSS 要件 12.3.1 に従って、カスタマイズアプローチで満たす各要件について、詳細なターゲットリスク分析を提供する必要があります。リスク分析では、リスクを定義し、定義された要件が満たされない場合のセキュリティへの影響を評価し、コントロールが定義された PCI DSS 要件によって提供されるのと少なくとも同等のレベルの保護を提供すると事業体が判断した方法を説明します。

評価者は、ターゲットリスク分析の情報を使用して、評価の計画および準備を行います。

カスタマイズアプローチのためのターゲットリスク分析を完了するにあたっては、以下の点を覚えておくことが重要です。

- 保護される資産は、事業体によって保存、処理、または伝送されるカード会員データです。
- 脅威の主体は、高い動機と能力を備えています。脅威行為者の動機と能力は、攻撃が成功した場合に実現するカード会員データの量に関連して増加する傾向があります。
- 事業体が脅威行為者の標的となる可能性は、事業体がより大量のカード会員データを保存、 処理、または送信するほど高くなります。
- 害悪は目的に直接関係します。例えば、目的が「悪意のあるソフトウェアが実行できないこと」であれば悪意のあるソフトウェアが実行されること、目的が「すべての活動を実行するための日々の責任が割り当てられていること」であれば責任が割り当てられていないことが害悪であると言えます。

注: *このターゲットリスク分析で使用される「mischief （害悪）」という用語（たとえば、下表の 1.3 において）は、事業体のセキュリティ体制にマイナスの影響を与える出来事またはイベントを指します。この例としては、ポリシーの不在、脆弱性スキャンの未実施、事業体の環境下でマルウェアが実行されることなどが挙げられます。*

このターゲットリスク分析テンプレートのサンプルは、事業体が文書化し、カスタマイズされた検証のために評価者に提供すべき最小限の情報を含んでいます。この特定のテンプレートを使用する必要はありませんが、事業者のカスタマイズアプローチ文書には、このテンプレートに定義されたすべての情報が含まれ、事業者はこの正確な情報を評価者に提供することが要求されます。

ターゲットリスク分析には、少なくとも以下の表の情報を含める必要があります。

カスタマイズアプローチを介して満たされた PCI DSS 要件のターゲットとなるリスク分析のサンプル 評価対象事業者が記入すること	
項目	**詳細**
1.要件の特定	
1.1 記述されている PCI DSS 要件を特定する。	<事業体が要件を特定します>
1.2 記述されている PCI DSS 要求の目的を特定する。	<事業体は、要件の目的を識別します>。
1.3 要件が防止するために設計された害悪を記述する	<事業体は、害悪を説明します>。 <事業体は、その目的がうまく満たされない場合、そのセキュリティへの影響を記述します>。 <事業体は、その目的がうまく満たされない場合、どのようなセキュリティの基礎が整備されないか、または脅威者が何をすることができるかを記述します>。

カスタマイズアプローチを介して満たされた PCI DSS 要件のターゲットとなるリスク分析のサンプル 評価対象事業者が記入すること	
項目	**詳細**
2.提案されたソリューションを記述する	
2.1 カスタマイズされたコントロールの名前／識別子	<コントロールマトリックスに記載されているカスタマイズされたコントロールを事業体が識別します>。
2.2 提案されたソリューションでは、記述されている要件のどの部分が変更されるか？	<事業体は、要求のどの要素が定義されたアプローチで満たされず、カスタマイズアプローチでカバーされるかを識別します。これは、要件の周期性を変更するような小さなものから、目的を達成するために全く異なるコントロールのセットを実装するようなものまであります。
2.3 提案されたソリューションは、どのように害悪を防ぐのか？	<事業体は、コントロールマトリクスに詳述されたコントロールが、1.3.で特定された害悪をどのように防ぐかを記述します>。
3.カード会員情報の機密保持違反につながる害悪の発生可能性の変化を分析する。	
3.1 コントロールマトリックスに詳述されている害悪の発生可能性に影響を与える要因を記述。	事業体が説明します。 • コントロールがどの程度、害悪を防ぐのに成功するか。 • コントロールマトリックスに詳述されているコントロールが、どのように害悪の発生可能性を低減させるか。

カスタマイズアプローチを介して満たされた PCI DSS 要件のターゲットとなるリスク分析のサンプル 評価対象事業者が記入すること						
項目	**詳細**					
3.2 カスタマイズされたコントロールの適用後にも害悪の発生可能性がある理由を記述。	事業体が説明します。 • コントロールが失敗する典型的な理由、その可能性、どのようにそれを防ぐことができるか。 • コントロールが正常に動作していないことを検出するために、事業体のプロセスとシステムはどの程度レジリエンスがあるか？ • 脅威者はどのようにこのコントロールを迂回することができるか - どのようなステップを踏む必要があるか、どの程度難しいか、コントロールが機能しなくなる前に脅威者は検知されるか？これはどのように決定されたか？					
3.3 カスタマイズアプローチで詳述されているコントロールは、定義されたアプローチの要件と比較して、害悪の発生可能性の変化をどの程度表しているか。	害悪が発生する可能性がより高い	☐	変化なし	☐	害悪が発生する可能性がより低い	☐
3.4 カスタマイズしたコントロールを導入した場合に、害悪が発生する可能性が変化すると評価する根拠を記入してください。	事業体が提供します。 • 3.3 で文書化した評価の正当な理由。 • 3.3.で文書化した評価に使用した基準および値。					

カスタマイズアプローチを介して満たされた PCI DSS 要件のターゲットとなるリスク分析のサンプル 評価対象事業者が記入すること				
項目	**詳細**			
4.アカウントデータへの不正アクセスの影響に関するあらゆる変更を分析する。				
4.1 このソリューションが対象とするシステムコンポーネントの範囲において、このソリューションが失敗した場合、不正アクセスのリスクとなるアカウントデータの量はどの程度か？	**4.1.1** 保存された PAN の数	*常時最大*	**4.1.2** 12 カ月間に処理または伝送された PAN の数	*合計*
4.2 カスタマイズされたコントロールが直接的にどのように役立つかについて説明する。 • 脅威者が成功した場合に、侵害される個々の PAN の数を減らす、および／または、脅威者が成功した場合に、侵害される個々の PAN の数を減らす。 • カードブランドに対して、漏洩した PAN を迅速に通知することができるようにする。	ペイメントエコシステムへの影響は、漏洩したアカウントの数と、漏洩した PAN をイシュアがどれだけ早くブロックできるかに直接関係します。 事業体は、カスタマイズされたコントロールがある場合、どのように以下を達成するかを説明します。 • 保存、処理、または伝送されるカード会員データの量を減らし、その結果、脅威の実行者が利用できる量 を減らす。 • 検出、漏洩したアカウントの通知、および脅威者の封じ込めまでの時間を短縮する。			
5.リスクの承認と見直し				
5.1 私は上記のリスク分析を検討し、提案されたカスタマイズアプローチを詳細に使用することで、該当する PCI DSS 要件の定義されたアプローチと少なくとも同等のレベルの保護が得られることに同意する。	経営層のメンバーは、提案されたカスタマイズアプローチをレビューし、これに同意する必要があります。 <事業体の経営層メンバーは、ここに文書化されたカスタマイズアプローチをレビューし、同意したことに署名します>。			

カスタマイズアプローチを介して満たされた PCI DSS 要件のターゲットとなるリスク分析のサンプル 評価対象事業者が記入すること	
項目	**詳細**
5.2 このリスク分析の見直しと更新は、遅くとも 1 年以内に行わなければならない。	リスク分析は、少なくとも 12 カ月ごとに見直す必要があり、カスタマイズアプローチ自体に時間的制限がある場合（例えば、技術の変更が予定されているため）、または他の要因によって必要な変更が指示された場合は、より頻繁に見直す必要があります。予定外のリスクレビューが行われた場合は、レビューが行われた理由を詳細に記述します。 <ターゲットリスク分析がレビューされ、更新された日を示す事業体>。

付録F　要件 6 をサポートするための PCI ソフトウェアセキュリティフレームワークの活用

PCI DSS 要件 6 では、安全なシステムおよびソフトウェアの開発および保守に関する要件が定義されています。PCI SSC セキュリティソフトウェア基準および セキュア SLC 基準（総称してソフトウェアセキュリティフレームワーク）には厳格なソフトウェアセキュリティ要件が含まれているため、いずれかの規格に従って開発および保守された特注およびカスタムソフトウェアを使用すると、事業体は追加の詳細テストを実行せずに PCI DSS 要件 6 のいくつかの要件を満たすことができ、他の要件に対するカスタマイズアプローチの使用もサポートされる場合があります。詳細については、表 7 を参照してください。

注：*要件 6 を満たすためのこのサポートは、セキュアソフトウェア基準またはセキュア SLC 基準に従って特別に開発および保守されるソフトウェアにのみ適用され、要件 6 の適用範囲の他のソフトウェアまたはシステムコンポーネントには適用されません。*

表 7.要件 6 をサポートするための PCI ソフトウェアセキュリティフレームワークの活用

PCI DSS の要件	セキュアソフトウェア基準に準拠して開発および保守されたソフトウェアに PCI DSS 要件が適用される方法	セキュア SLC 基準に従って開発および保守されるソフトウェアに PCI DSS 要件が適用される方法
6.1 要件 6 の活動を行うためのプロセスおよび仕組みが定義され、理解されている。	PCI DSS 要件／目標が通常通り適用されます。	
6.2 特注ソフトウェアおよびカスタムソフトウェアが安全に開発される。	PCI DSS 要件 6.2.4 は、セキュアソフトウェア基準に従って開発および保守されるソフトウェアに適用されると考えることができます。	PCI DSS 要件 6.2 は、セキュア SLC 基準に従って開発および保守されるソフトウェアに対して設定されていると見なすことができます。

PCI DSS の要件	セキュアソフトウェア基準に準拠して開発および保守されたソフトウェアに PCI DSS 要件が適用される方法	セキュア SLC 基準に従って開発および保守されるソフトウェアに PCI DSS 要件が適用される方法
6.3 セキュリティの脆弱性が特定され、速やかに対処されている。	PCI DSS 要件／目標が通常通り適用されます。 セキュア SLC 基準に従って開発および保守されたソフトウェアは、要件 6.3 の目標に対するカスタマイズアプローチをサポートする場合があります。 セキュア SLC 基準に従って開発および保守されたソフトウェアを使用すると、ベンダがセキュリティパッチおよびソフトウェア更新をタイムリーに提供することが保証されますが、パッチおよび更新が PCI DSS 要件に従ってインストールされることを**保証する責任は事業体**が保持します。	
6.4 公衆向けの ウェブアプリケーションが攻撃から保護されている。	PCI DSS 要件／目標が通常通り適用されます。	
6.5 すべてのシステムコンポーネントへの変更が安全に管理されている 。	PCI DSS 要件／目標が通常通り適用されます。 セキュア SLC 基準に従って開発および保守されたソフトウェアは、要件 6.5 の目標に対するカスタマイズアプローチをサポートする場合があります。 セキュア SLC 基準に従って開発および保守されたソフトウェアを使用すると、ベンダがソフトウェアおよび関連 更新の開発中に変更管理手順に従うことが保証されますが、システムコンポーネントに対するソフトウェアおよびその他の変更が PCI DSS 要件に従って本番環境に実装されることを**保証する責任は事業体**が保持します。	

*セキュア**SLC** 認定ベンダによって開発および保守された特注およびカスタムソフトウェアの使用*

PCI DSS 要件 6.2 を満たし、要件 6.3 および 6.5 のカスタマイズアプローチをサポートするためにセキュア SLC 認定ベンダが開発および保守するソフトウェアの使用を検証する場合、評価者は以下を満たしていることを確認する必要があります。

- ソフトウェアベンダが PCI SSC の セキュア SLC 認定ベンダリストに現在登録されている（つまり、検証の有効期限が切れていない）。
- ソフトウェアは、ソフトウェアベンダの検証の一部として評価されたソフトウェアライフサイクル管理手法を使用して開発され、維持されている。
- セキュア SLC 認定ベンダが提供する実装ガイダンスに従っている。

*セキュア **SLC** 基準に準拠して開発された特注ソフトウェアおよびカスタムソフトウェアの使用*

自社で使用するソフトウェアのみを開発する事業者、または単一の事業者が使用するソフトウェアを開発する事業者は、SLC アセッサに依頼して、自社のソフトウェアライフサイクル管理慣行を SLC 規格に照らして評価することができます。セキュア SLC 評価者は、評価結果をセキュア SLC 適合性報告書（ROC）およびセキュア SLC 適合性証明書（AOC）として文書化します。

ソフトウェアライフサイクル管理の実践に従って開発および保守されるソフトウェアは、セキュア SLC 認定ベンダによって開発および保守されるソフトウェアと同様に PCI DSS 要件 6 をサポートします。これらの実践が セキュア SLC 評価者によって評価され、セキュア SLC 基準の要件を満たすことが確認されて、その結果がセキュア SLC ROC および AOC に文書化された場合、SLC 認定ベンダはこれらの実践をサポートします。

*セキュア **SLC** 規格の使用状況の検証*

PCI DSS 要件 6.2 を満たし、要件 6.3 および 6.5 のカスタマイズアプローチをサポートするために セキュア SLC 基準に従って開発および保守されたソフトウェアの使用を検証する場合、評価者は以下を満たしていることを確認する必要があります。

- ソフトウェアライフサイクル管理方法がセキュア SLC 評価者によって評価され、セキュア SLC 基準のすべての要件を満たすことが確認され、その結果がセキュア SLC 準拠報告書（ROC）および セキュア SLC 準拠証明書（AOC）に文書化されていること。
- このソフトウェアは、セキュア SLC 評価の対象となるソフトウェアライフサイクル管理手法を使用して開発および保守されていること。

- ソフトウェアライフサイクルマネジメントの実践に関する完全なセキュア SLC 評価が過去 36 カ月以内に完了した。さらに、直近の完全なセキュア SLC 評価が 12 カ月以上前に実施された場合、開発者／ベンダが過去 12 カ月以内に、使用中のソフトウェアライフサイクル管理手法に関してセキュア SLC 基準を継続して順守していることを確認する年次証明書を提供したこと。

セキュアソフトウェア基準の使用状況の確認

PCI DSS 要件 6.2.4 を満たし、要件 6.3 および 6.5 のカスタマイズアプローチをサポートするために、セキュアソフトウェア基準に従って開発および保守されたソフトウェアの使用を検証する場合、評価者は以下を満たしていることを確認する必要があります。

- セキュアソフトウェア評価者がセキュアソフトウェア評価を実施し、その結果がセキュアソフトウェア検証報告書（ROV）およびセキュアソフトウェア準拠証明書（AOV）に文書化され、セキュアソフトウェア規格のすべての要件を満たすことが確認されたこと。
- このソフトウェアは、セキュアソフトウェア評価で対象となったソフトウェアライフサイクル管理手法で開発され、維持されていること。
- 過去 36 カ月以内にセキュアソフトウェアの完全な評価が完了した。さらに、直近の完全なセキュアソフトウェア評価が 12 カ月以上前に行われた場合、セキュアソフトウェア規格を継続して順守していることを確認する年次証明書が、過去 12 カ月以内に開発者／ベンダによって提供されたこと。

付録G　PCI DSS 用語集、略語、頭字語

用語	定義
AES	「アドバンストエンクリプションスタンダード」の頭字語です。 *強力な暗号化技術*を参照してください。
ANSI(アンシ)	「アメリカ国家規格協会」の頭字語です。
AOC	「準拠証明書」の頭字語です。AOC は、コンプライアンスに関する自己問診または報告書に記録されている通り、加盟店およびサービスプロバイダが PCI DSS 評価結果を証明するための文書です。
ASV	「承認されたスキャニングベンダ」の頭字語です。 PCI SSC が外部脆弱性スキャンサービスを実施することを承認した企業です。
BAU	「通常通りのビジネス」の頭字語 BAU は会社の通常通りの日常ビジネス業務です。
CDE	「カード会員データ環境」の頭字語。 CDE は以下のもので構成されます。 • カード会員データまたは機密認証データを保存、処理、または伝送するシステムコンポーネント、人、および プロセスです。 • カード会員データ（CHD）／機密認証データ（SAD）を保存、処理、または伝送しないが、カード会員データ（CHD)／機密認証データ（SAD）を保存、処理、または伝送するシステム・コンポーネントに無制限の接続性を有するシステム・コンポーネントです。
CERT	「コンピュータ緊急対応チーム」の頭字語です。
CIS	「インターネットセキュリティセンター」の頭字語です。
CVSS	「共通脆弱性スコアリングシステム」の頭字語です。 詳しくは、*ASV プログラムガイド*を参照してください。
DMZ	「非武装地帯」の略語です。 事業体内部のプライベートネットワークに追加のセキュリティ層を提供する、物理的または論理的なサブネットワークです。
DNS	ドメインネームシステムの頭字語です。

用語	定義
ECC	「楕円曲線暗号」 の頭字語です。 *「強力な暗号化技術」*を参照してください。
E コマース（ウェブ）リダイレクトサーバ	e コマース取引の際、決済処理のために顧客のブラウザをマーチャントのウェブサイトから別の場所にリダイレクトさせるサーバのことです。
FTP	ファイル転送プロトコルの頭字語です。 インターネットなどの公衆ネットワークを通じて、あるコンピュータから別のコンピュータにデータを転送するために使用されるネットワークプロトコルです。FTP は、パスワードやファイルの内容が保護されずに平文で送信されるため、安全でないプロトコルとして広く認識されています。FTP は、SSH やその他の技術によって安全に実装することができます。
HSM	「ハードウェアセキュリティモジュール」または「ホストセキュリティモジュール」の頭字語です。 暗号鍵管理機能および／またはアカウントデータの復号に使用される、安全な暗号サービスのセットを提供する、物理的および論理的に保護されたハードウェアデバイスです。
IDS	「侵入検知システム」の頭字語です。
IPS	「侵入防御システム 」の頭字語です。
ISO	「国際標準化機構」の頭字語です。
LAN	「ローカルエリアネットワーク」の頭字語です。
LDAP	「ライトウェイトディレクトリアクセスプロトコル 」の頭字語です。
MAC	暗号技術において、「メッセージ認証コード」の頭字語です。 *「強力な暗号化技術」*を参照してください。
MO/TO	「メールオーダー／テレフォンオーダー」の頭字語です。
NAC	「ネットワークアクセスコントロール」の頭字語です。
NAT	ネットワークアドレス変換の頭字語です。

用語	定義
NIST	「国立標準技術研究所」の頭字語です。 米国国立標準技術研究所内の非規制連邦機関、米国商務省技術局内の非規制連邦機関です。
NTP	「ネットワークタイムプロトコル」の頭字語です。
OWASP	「オープンウェブ アプリケーションセキュリティプロジェクト」の頭字語です。
PAN	「プライマリアカウント番号（Primary Account Number）」の頭字語で、「アカウント番号」とも呼ばれます。イシュアおよび特定のカード会員アカウントを識別する、一意なカード番号（一般に、クレジットカードまたはデビットカード）です。
PCI DSS	「ペイメントカード業界データセキュリティ基準」の頭字語です。
PIN	「個人識別番号」の頭字語です。
PIN ブロック	処理中に PIN をカプセル化するために使用されるデータブロックです。PIN ブロック形式は、PIN ブロックの内容と、PIN を取り出すための処理方法を定義します。PIN ブロックは PIN と PIN 長から構成され、使用する ISO PIN ブロック形式によっては PAN（またはその切り捨て）を含むことがあります。
POI	「加盟店端末装置（Point of Interaction）」の頭字語です。カードからデータを読み取る最初のポイントです。POI は、ハードウェアとソフトウェアで構成される電子取引認識製品であり、カード会員がカード取引を行うことができるようにするために認識装置でホストされます。POI は有人の場合と無人の場合があります。一般に、POI トランザクションは IC（チップ）カードまたは磁気ストライプカード（あるいはその両方）を使用したペイメントトランザクションです
POS	加盟店が顧客から支払いを受けるために使用するハードウェアおよびソフトウェア。POI デバイス、PIN パッド、電子レジスターなどが含まれる場合がある。
QIR	「認定インテグレーター」または「リセラー」の頭字語です。 詳細については、PCI SSC ウェブサイトの *QIR プログラムガイド*を参照してください。
QSA	認定セキュリティ評価者の頭字語です。 QSA は、PCI SSC が PCI DSS オンサイト評価を実施するための資格を有します。QSA 企業および従業員の要件の詳細については、「*QSA 資格要件*」を参照してください。

用語	定義
RSA	公開鍵暗号のアルゴリズムです。*「強力な暗号化技術」*を参照してください。
SAQ	「自己問診 (Self-Assessment Questionnaire)」の頭字語です。事業体の PCI DSS 評価からの自己問診結果を文書化するために使用するレポートツールです。
SNMP	「簡易型ネットワーク管理プロトコル」の頭字語の頭字語です。
SQL	「構造化照会言語」の頭字語です。
SSH	「セキュアシェル」の略語です。
SSL	「セキュアソケットレイヤー」の頭字語です。
TDES	「トリプルデータ暗号化規格」の頭字語です。 3DES」または「トリプル DES」とも呼ばれます。
TLS	「トランスポートレイヤーセキュリティ」の頭字語です。
VPN	「仮想プライベートネットワーク」 の頭字語です。
アカウント	「ユーザ ID」、「アカウント ID」、「アプリケーション ID」とも呼ばれます。 コンピュータ・システム上で個人またはプロセスを識別するために使用される。*認証クレデンシャル*および*認証ファクタ*を参照してください。
アカウントデータ	アカウントデータは、カード会員データおよび／または機密認証データから構成されます。*カード会員情報*と*機密認証データ*を参照してください。
アクワイアラ	「マーチャントバンク」、「アクワイアリングバンク」、「アクワイアリング金融機関」とも呼ばれます。 加盟店のためにペイメントカード取引を処理する事業体（通常は金融機関）で、ペイメントブランドによってアクワイアラとして定義されています。アクワイアラは、加盟店のコンプライアンスに関するペイメントブランドの規則と手続きの対象となります。*ペイメントプロセッサー*をご参照ください。
アプリケーション	内部および外部（例えば、ウェブ）アプリケーションを含む、すべての購入、カスタム、および特注のソフトウェアプログラムまたはプログラム群を含みます。

用語	定義
アプリケーションとシステムアカウント	「サービスアカウント」とも呼ばれます。 コンピュータシステムまたはアプリケーションでプロセスを実行したり、タスクを実行したりするアカウントです。これらのアカウントは通常、特殊なタスクや機能を実行するために必要な高い権限を持ち、通常、個人で使用するアカウントではありません。
アンチマルウェア	様々な形態の悪意のあるソフトウェアを検出し、削除、ブロック、または封じ込めるように設計されたソフトウェアです。
インタラクティブ・ログイン	個人が認証情報を提供して、アプリケーションまたはシステムアカウントに直接ログインするプロセスです。
インデックス・トークン	ある PAN に対応するランダムな値のテーブルからのランダムな値です。
ウェブアプリケーション	一般的にウェブ ブラウザやウェブ サービスを通じてアクセスするアプリケーションのことです。ウェブ アプリケーションは、インターネットまたはプライベートな内部ネットワークを通じて利用することができます。
事業体	PCI DSS の評価を受ける事業体、組織、または事業を表すために使用される用語です。
オーダーメイドとカスタムソフトウェアのこと。	*オーダーメイドのソフトウェア*は、事業体のために、事業体の仕様に従って第三者が開発したものです。 *カスタムソフトウェア*は、事業体が自社で使用するために開発するものです。
カードスキマー	ペイメントカードから情報を不正に取得および／または保存するために設計された、正規のカード読取装置に取り付けられることの多い物理的な装置です。
カード会員	ペイメントカードの発行先である顧客、またはペイメントカードの使用を許可された個人です。
カード会員データ	カード会員情報は、最低でも全桁数の PAN で構成されます。カード会員データは、全桁数の PAN に、カード会員名、有効期限、サービスコードのいずれかを加えた形式で表示されることもあります。 ペイメントトランザクションの一部として送信または処理される（ただし保存されない）その他のデータ要素については、*機密認証データ*を参照してください。

用語	定義
カード検証コード	カードバリデーションコードまたはバリュー、カードセキュリティコードとも呼ばれる。PCI DSS の目的では、ペイメントカードの表面または裏面に印刷された 3 桁または 4 桁の値のことです。参加ペイメントブランドによっては、CAV2、CVC2、CVN2、CVV2、CID と表記されることもあります。詳細については、参加ペイメントブランドにお問い合わせください。
カスタマイズアプローチ	*PCI DSS 編：PCI DSS の導入と検証のための 8 つのアプローチ」を参照。*
カラムレベルデータベース暗号化	データベース内の特定の列の内容を、データベース全体の全内容と比較して暗号化する技術です（ソフトウェアまたはハードウェアのいずれか）。または、*ディスク暗号化*、*ファイルレベル暗号化*も参照してください。
クリアテキストデータ	暗号化されていないデータです。
クリティカルシステム	事業者が特に重要であると判断したシステムまたは技術のことです。例えば、重要なシステムは、事業活動の遂行やセキュリティ機能の維持に不可欠である場合があります。重要なシステムの例としては、セキュリティシステム、公衆向けのデバイスとシステム、データベース、 カード会員データを保存、処理、または伝送するシステムなどがよく挙げられます。
コンソール	サーバ、メインフレームコンピュータ、またはその他のシステムタイプにアクセスし、制御することを可能にする、直接接続された画面および／またはキーボードです。*ノンコンソールアクセス*を参照してください。
サードパーティサービスプロバイダ(TPSP)	事業体に代わってサービス提供者として活動するあらゆる第三者です。*マルチテナントサービスプロバイダ*、*サービスプロバイダ*を参照してください。
サードパーティソフトウェア	事業体によって取得されるが、事業体のために明示的に開発されたのではないソフトウェアです。オープンソース、フリーウェア、シェアウェア、または購入したものです。
サービスコード	ペイメントカードの有効期限に続く磁気ストライプのトラックデータ上の 3 桁または 4 桁の値です。サービス属性の定義、国際・国内インターチェンジの区別、利用制限の識別など、様々なことに使われます。

用語	定義
サービスプロバイダ	ペイメントブランドではない、他の事業体に代わってカード会員データの処理、保存、送信に直接関与する事業体です。これには、ペイメントゲートウェイ、ペイメントサービスプロバイダ（PSP）、独立販売組織（ISO）が含まれます。これにはカード会員データのセキュリティを制御する、または影響を与える可能性のあるサービスを提供する企業も含まれます。例としては、マネージドファイアウォール、IDS、その他のサービスを提供するマネージドサービスプロバイダ、ホスティングプロバイダ、その他の事業者が挙げられます。 通信会社が通信リンク*のみ*を提供するなど、公共ネットワークアクセスの提供のみを伴うサービスを提供する場合、その企業はそのサービスのサービスプロバイダとはみなされません（他のサービスについてはサービスプロバイダとみなされる可能性があります）。*マルチテナントサービスプロバイダ*、*サードパーティサービスプロバイダ*を参照してください。
システムレベルオブジェクト	システムコンポーネント上のもので、その動作に必要なものです。アプリケーション実行ファイルと設定ファイル、システム設定ファイル、静的ライブラリと共有ライブラリと DLL、システム実行ファイル、デバイスドライバとデバイス設定ファイル、およびサードパーティコンポーネントを含むが、これに限定されません。
システム構成要素	カード会員データ環境（CDE）に含まれる、またはカード会員データ環境（CDE）に接続されるネットワーク機器、サーバ、コンピューティングデバイス、仮想コンポーネント、ソフトウェア、またはカード会員データ環境（CDE）のセキュリティに影響を与える可能性があるものです。
適用範囲	PCI DSS 評価に含まれるすべてのシステムコンポーネント、人、およびプロセスを特定するプロセスです。*PCI DSS 要件とセキュリティ評価手順*の「PCI DSS 要件の範囲」を参照してください。
スプリットナレッジ	2 つ以上の事業体が別々にキーコンポーネントまたはキーシェアを持ち、個々に結果の暗号鍵に関する知識を伝えない方法です。
セキュアコーディング	改ざんや漏洩に強いアプリケーションを作成し、実装するプロセスです。
セキュリティイベント	システムまたはその環境に対してセキュリティ上の影響を及ぼす可能性があると事業体が考える出来事。PCI DSS の文脈では、セキュリティイベントは疑わしい活動や異常な活動を特定します。
セキュリティ責任者	事業体のセキュリティに対する主要な責任者です。

用語	定義
セグメンテーション	"ネットワーク・セグメンテーション "または "アイソレーション "とも呼ばれる。セグメンテーションは、カード会員データを保存、処理、または伝送するシステムコンポーネントを、そうでないシステムから分離するものです。PCI DSS のセクションの「セグメンテーション」を参照してください。4 PCI DSS 要件の範囲」の「セグメンテーション」を参照してください。
センシティブエリア	センシティブエリアは、通常カード会員データ環境（CDE）のサブセットであり、カード会員データ環境（CDE）にとって重要であると考えられるシステムを収容するあらゆるエリアを指します。これには、データセンター、サーバルーム、小売店のバックオフィスルーム、カード会員データの保存、 処理、伝送が集中または集約されているエリアが含まれます。機密エリアには、カード会員データ環境（CDE）のセキュリティを管理または維持するシステム（たとえば、ネットワークセキュリティ制 御または物理的または論理的セキュリティを管理するシステム）が収容されているエリアも含まれます。 小売店のキャッシャーエリアや、エージェントが支払いを受けるコールセンターなど、POS 端末のみが存在するエリアは除きます。
機密認証データ(SAD)	カード会員をオーソリゼーションするため、および／またはペイメントカード取引を承認するために使用されるセキュリティ関連情報です。この情報には、カード検証コード／値、（磁気ストライプまたは同等のチップからの）フルトラックデータ、PIN、および PIN ブロックが含まれますが、これらに限定されるものではありません。
テルネット	「電話回線網プロトコル」の略語です。
データフロー図	アプリケーション、システム、またはネットワークを通じてデータがどのように流れるかを示す図です。
ディスク暗号化	デバイス（ハードディスクやフラッシュドライブなど）上のすべての保存データを暗号化するための技術です（ソフトウェアまたはハードウェア）。また、特定のファイルや列の内容を暗号化するために、ファイルレベル暗号化または列レベルデータベース暗号化も使用されます。
デフォルトのパスワード	システム、アプリケーション、またはデバイスにあらかじめ定義されたシステム管理、ユーザ、またはサービスアカウントに関するパスワードです。通常はデフォルトアカウントに関連付けられます。デフォルトのアカウントとパスワードは公開されており、よく知られているため、容易に推測されます。

用語	定義
デフォルトアカウント	システム、アプリケーション、またはデバイスにあらかじめ定義されたログインアカウントで、システムを初めて使用するときに最初のアクセスを許可します。インストールプロセスの一部として、追加のデフォルトアカウントがシステムによって生成されることもあります。
デュアルコントロール	機密性の高い機能または情報を保護するために、2 つ以上の別々の主体（通常は個人）が協調して動作するプロセスです。両主体は、脆弱な取引に関わる物質の物理的保護に等しく責任を負います。一人の人間が材料（例えば、暗号鍵）にアクセスしたり、使用したりすることは許されない。手動による鍵の生成、運搬、積込み、保管、および取り出しの場合、デュアルコントロールでは、鍵の知識を各事業体に分割することが必要です。*「スプリットナレッジ」*を参照してください。
トークン	認証とアクセス制御の文脈では、トークンは、認証サーバまたは VPN と連携して動的認証または多要素認証を実行するハードウェアまたはソフトウェアによって提供される値です。
トラックデータ	「フルトラックデータ」または「磁気ストライプデータ」とも呼ばれます。 決済取引時にオーソリゼーションおよび認可のために使用される磁気ストライプまたはチップに符号化されたデータ。チップ上の磁気ストライプイメージまたは磁気ストライプ上のトラックデータである可能性があります。
トランケーション	PAN データのセグメントを削除することにより、完全な PAN を読めなくする方法です。電子的に保存、処理、伝送される場合の PAN の保護に関連します。 画面や紙の領収書などに表示される PAN の保護については、*マスキング*を参照のこと。
ネットワークセキュリティコントロールズ (NSC)	ファイアウォールなどのネットワークセキュリティ技術で、ネットワークポリシーの実施点として機能します。NSC は通常、事前に定義されたポリシーまたはルールに基づいて、2 つ以上の論理的または物理的なネットワークセグメント（またはサブネット）間のネットワークトラフィックを制御します。
ネットワーク図	ネットワーク環境内のシステムコンポーネントと接続を示す図です。
ネットワーク接続	ネットワーク層のパケットの送受信を可能にする、機器間の論理的、物理的、または仮想的な通信経路のことです。
ノンコンソールアクセス	システムコンポーネントへの直接的、物理的な接続ではなく、ネットワークインターフェイスを介して行われる、システムコンポーネントへの論理的なアクセスです。コンソール以外のアクセスには、ローカル／内部ネットワークからのアクセスと、外部またはリモートネットワークからのアクセスが含まれます。

用語	定義
ハッシュ化	データを固定長のメッセージダイジェストに変換して保護する方法です。ハッシュは、非機密のアルゴリズムが任意の長さのメッセージを入力とし、固定長の出力（通常「ハッシュコード」または「メッセージダイジェスト」と呼ばれる）を生成する一方通行（数学）関数です。ハッシュ関数には、以下のような性質が求められます。 • ハッシュコードのみから元の入力を決定することは計算上不可能であること。 • 同じハッシュコードを与える 2 つの入力を見つけることは計算上不可能であること。
パスワード／パスフレーズ	ユーザまたはアカウントの認証要素となる文字列です。
パッチ	既存のソフトウェアに機能追加や不具合を修正するためのアップデートです。
ファイアウォール	ネットワークリソースを不正なアクセスから保護するためのハードウェアおよび／またはソフトウェア技術です。ファイアウォールは、一連のルールやその他の基準に基づいて、異なるセキュリティレベルのネットワーク間でコンピュータのトラフィックを許可または拒否します。
ファイルレベルの暗号化	特定のファイルの全内容を暗号化するための技術です（ソフトウェアまたはハードウェア）。*ディスク暗号化*と*列レベルのデータベース暗号化*を参照することもできます。
ファイル整合性監視 (FIM)	重要なファイルの変更、追加、削除をチェックし、変更を検出した場合に通知する変更検出ソリューションです。
フォレンジック	"コンピュータフォレンジック "とも呼ばれます。 情報セキュリティに関連して、データ侵害の原因を特定するために、コンピュータ資源から証拠を収集する調査ツールや分析技術を適用することです。 支払データの漏洩に関する調査は、通常、PCI 法科学捜査官（PFI）によって実施されます。
ペイメントカードのフォームファクタ	物理的なペイメントカードと、ペイメントカードをエミュレートして決済取引を開始する機能を持つデバイスが含まれます。このようなデバイスの例としては、スマートフォン、スマートウォッチ、フィットネスバンド、キータグ、ジュエリーなどのウェアラブルなどが挙げられますが、これらに限定されるものではありません。

用語	定義
ペイメントブランド	ペイメントカードやその他のペイメントカードのフォームファクターをブランド化した事業体。ペイメントブランドは、そのブランドまたはロゴが付いたペイメントカードまたは他のフォームファクタが使用される場所と方法を規制します。ペイメントブランドは、PCI SSC 参加ペイメントブランド、またはその他のグローバルもしくは地域のペイメントブランド、スキーム、またはネットワークである場合があります。
ペイメントプロセッサー	「ペイメントゲートウェイ」または「ペイメントサービスプロバイダ（PSP）」と呼ばれることもあります。 ペイメントカード取引を代行するために、マーチャントまたはその他の事業者が契約する事業者です。 *アクワイアラ*を参照してください。
決済ページ	消費者からアカウントデータを取得する、または取得したアカウントデータを送信することを目的とした 1 つまたは複数のフォーム要素を含むウェブベースのユーザインターフェースです。決済ページは、以下のいずれかとしてレンダリングすることができます。 • 単一のドキュメントまたはインスタンス。 • 非決済ページ内のインラインフレームに表示される文書またはコンポーネント。 • 非決済ページ内の複数のインラインフレームに含まれる、それぞれが 1 つ以上のフォーム要素を含む複数の文書またはコンポーネント。
加盟店	PCI DSS の目的では、加盟店とは、PCI SSC 参加ペイメントブランドのロゴが付いたペイメントカードを商品やサービスに対する支払いとして受け入れるあらゆる事業体と定義されます。 商品および／またはサービスの支払いとしてペイメントカードを受け入れる加盟店は、販売したサービスが他の加盟店またはサービスプロバイダに代わってカード会員データを保存、処理、または送信するものである場合、サービスプロバイダである可能性もあります。たとえば、ISP は毎月の請求のためにペイメントカードを受け付ける加盟店ですが、加盟店を顧客として受け入れる場合は、サービスプロバイダでもあります。
マスキング	PAN のセグメントを表示または印刷する際に隠す方法です。マスキングは、ビジネス上 PAN 全体を表示する必要がない場合に使用されます。マスキングは、画面、紙の領収書、印刷物などに表示される PAN の保護に関連します。 電子的に保存、処理、送信される場合の PAN の保護については、*トランケーション*を参照してください。

用語	定義
マルチテナントサービスプロバイダ	システムリソース（物理サーバーや仮想サーバーなど）、インフラ、アプリケーション（SaaS を含む）、データベースなどを共有し、加盟店や他のサービスプロバイダーに対してさまざまな共有サービスを提供するサードパーティサービスプロバイダーの一種。サービスには、単一の共有サーバー上での複数のエンティティのホスティング、電子商取引および/または「ショッピングカート」サービスの提供、Web ベースのホスティングサービス、決済アプリケーション、様々なクラウドアプリケーションおよびサービス、および決済ゲートウェイとプロセッサへの接続が含まれますが、これらに限定されるものではありません。サービスプロバイダ」及び「サードパーティサービスプロバイダ」をご参照ください。
メディア	電子記憶装置、リムーバブル電子メディア、および紙の報告書を含むが、これらに限定されない物理的なマテリアルです。
リスクアセスメント	貴重なシステムリソースと脅威を特定し、発生の推定頻度とコストに基づいて損失エクスポージャー（つまり損失の可能性）を定量化し、（オプションとして）エクスポージャーの総額を最小限に抑えるための対策にリソースを割り当てる方法を推奨する、事業体全体のプロセスです。*ターゲットリスク分析*を参照してください。
リスクランキング	リスクを分類し、重要性の高い順に項目を特定し、優先順位をつけて対処するプロセスです。
リムーバブル電子メディア	デジタル化されたデータを保存するメディアで、あるコンピュータシステムから別のコンピュータシステムに容易に取り出したり、持ち運んだりすることができるものです。リムーバブル電子メディアの例としては、CD-ROM、DVD-ROM、USB フラッシュドライブ、外付け／ポータブルハードドライブなどがあります。この文脈では、取り外し可能な電子メディアには、ホットスワップ可能なドライブ、一括バックアップに使用されるテープドライブ、またはデータをある場所から別の場所で使用するために輸送するために通常使用されないその他のメディアは含まれません。
リモートアクセス	ネットワーク外から事業体のネットワークにアクセスすることです。リモートアクセスのための技術の例として、VPN があります。
ログ	*監査ログ*を参照してください。
ROC	「コンプライアンス報告書」の頭字語です。 事業体の PCI DSS 評価の詳細な結果を文書化するために使用される報告ツールです。

用語	定義
暗号キー	暗号アルゴリズムと組み合わせて使用されるパラメータで、次のような操作に使用されます。 • 平文データを暗号文データに変換する。 • 暗号文データを平文データに変換すること。 • データから計算されたデジタル署名。 • データから計算されたデジタル署名を検証すること。 • データから計算された認証コード、または • 共有秘密の交換契約。 *強力な暗号化技術*を参照してください。
暗号化	暗号アルゴリズムによってデータを（可逆的に）変換して暗号文を生成すること、すなわちデータの情報内容を隠すことです。*「強力な暗号化技術」*を参照。
暗号化アルゴリズム	"暗号化アルゴリズム "とも呼ばれます。 平文データを暗号化されたデータに変換するため、またはその逆のために使用される、明確に指定された可逆的な数学的プロセスです。*強力な暗号化技術*を参照してください。
暗号化アルゴリズム	*暗号化アルゴリズム*を参照してください。
暗号期間	暗号鍵が定義された目的のために使用できる時間帯です。多くの場合、鍵が有効な期間と鍵によって生成された暗号文の量によって定義され、業界のベストプラクティスやガイドライン（例えば、*NIST 特別刊行物 800-57*）に従って定義されています。
暗号鍵の管理	暗号鍵の確立および維持（必要に応じて古い鍵を新しい鍵に置き換えることを含む）を支援する一連のプロセスおよびメカニズムです。

用語	定義
暗号鍵の生成	鍵の生成は、鍵管理の中の機能の 1 つです。以下の文書は、適切な鍵の生成に関する公認のガイダンスを提供しています。 • *NIST 特別刊行物 800-133:暗号鍵生成のための推奨事項* • *ISO 11568-2 金融サービス - 鍵管理 (小売) - パート 2:対称型暗号、その鍵管理およびライフサイクル* – 4.3 鍵の生成 • *ISO 11568-4 金融サービス - 鍵管理（小売） - 第 4 部:非対称暗号システム - 鍵の管理およびライフサイクル* – 6.2 鍵のライフサイクル段階 - 生成 • *欧州決済理事会 EPC 342-08 アルゴリズムの使用および鍵管理に関するガイドライン* – 4.1.1 鍵の生成 [対称型アルゴリズムの場合] 4.1.1 鍵の生成 ［対称型アルゴリズムの場合 – 4.2.1 鍵の生成[非対称アルゴリズムの場合] 4.2.1 鍵の生成[非対称アルゴリズムの場合]。
仮想化	コンピューティングリソースを物理的および／または論理的な制約から論理的に抽象化することです。一般的な抽象化の 1 つは、仮想マシンまたは VM と呼ばれるもので、物理マシンの内容を取り込み、異なる物理ハードウェア上や同じ物理ハードウェア上の他の仮想マシンと一緒に動作させることができます。その他の一般的な抽象化には、コンテナ、サーバレスコンピューティング、またはマイクロサービスが含まれますが、これらに限定されるものではありません。
仮想決済端末	自己問診（SAQ）C-VT の文脈では、仮想決済端末とは、ペイメントカード取引を承認するためにアクワイアラ、プロセッサー、またはサードパーティサービスプロバイダのウェブサイトにウェブブラウザでアクセスし、加盟店がウェブブラウザを介してペイメントカードデータを手動で入力することを指します。物理的な端末とは異なり、仮想決済端末はペイメントカードから直接データを読み取ることはない。ペイメントカード取引は手動で入力されるため、仮想決済端末は通常、取引量の少ない加盟店環境で物理端末の代わりに使用されます。
監査ログ	「監査証跡」とも呼ばれる。 システムの活動を時系列に記録したものです。ある取引における操作、手順、または事象を取り巻く、またはそれにつながる一連の環境および活動を、開始から最終結果まで、再構築、レビュー、および調査するのに十分な、独立した検証可能な証跡を提供します。

用語	定義
管理者アクセス	システム、ネットワーク、および／またはアプリケーションを管理するために、そのアカウントに与えられた昇格または増加した特権です。 管理者アクセス権は、個人のアカウントまたはビルトインシステムのアカウントに割り当てられることがあります。管理アクセスを持つアカウントは、特定のオペレーティングシステムや組織構造に応じて、「スーパーユーザ」、「ルート」、「管理者」、「admin」、「sysadmin」、または「スーパーバイザ状態」と呼ばれることがよくあります。
危殆化	「データ漏洩」または「データ侵害」とも呼ばれます。 カード会員データの不正な開示／盗難、改ざん、破壊が疑われるコンピュータシステムへの侵入です。
強力な暗号化技術	暗号は、可逆的な暗号化プロセスを通じてデータを保護する方法であり、多くのセキュリティプロトコルやサービスで使用される基礎的なプリミティブです。強力な暗号化技術は、業界でテストされ受け入れられているアルゴリズムと、最低 112 ビットの有効な鍵長、および適切な鍵の管理方法に基づいています。 有効な鍵の強度は実際の鍵の「ビット」長よりも短くすることができます。そのため、より大きな鍵を持つアルゴリズムは、実際の鍵のサイズは小さいが有効な鍵のサイズがより大きいアルゴリズムよりも保護が弱くなる可能性があります。 *すべての新しい実装では、最低でも 128 ビットの有効鍵強度を使用することが推奨されています。* 暗号アルゴリズムと鍵長に関する業界の参考文献の例としては、以下のようなものがあります。 • *NIST 特別刊行物 800-57 第 1 部,* • *BSI TR-02102-1,* • *ECRYPT-CSA D5.4 アルゴリズム、鍵のサイズ、プロトコルのレポート(2018 年)、および* • ISO/IEC 18033 暗号化アルゴリズム、および • *ISO/IEC 14888-3:2-81 IT セキュリティ技術 - 付録付きデジタル署名 - 第 3 部：離散対数ベースのメカニズム ISO*
ペイメントカード	PCI DSS の目的では、PCI SSC 参加支払ブランドのロゴが付いた支払カードのフォームファクタを指します。
ペイメントチャネル	加盟店が顧客からの支払いを受け入れるために使用する方法。一般的な決済チャネルは、カードプレゼントの場合（対面）とカードが存在しない場合（電子商取引や MO/TO）です。

用語	定義
決済ページスクリプト	消費者のブラウザによって処理および／または解釈される、決済ページ上のあらゆるプログラミング言語のコマンドまたは命令です（ページのドキュメントオブジェクトモデルと相互作用するコマンドまたは命令を含む）。マークアップ言語（HTML など）やスタイルルール（CSS など）はプログラミング言語ではありません。
鍵管理システム	ハードウェアとソフトウェアの組み合わせで、デバイスやアプリケーションの暗号鍵を生成、配布、管理するための統合的なアプローチを提供するものです。
鍵管理者	秘密鍵、秘密鍵、キーシェア、またはキーコンポーネントに関する鍵管理の職務を、ある事業体に代わって行うことを委任され、かつその責任を負う者としての役割です。
鍵付き暗号ハッシュ	ランダムに生成される秘密鍵を組み込んだハッシュ関数で、ブルートフォース攻撃への耐性と秘密認証の完全性を提供します。 適切な鍵暗号ハッシュアルゴリズムには、以下のものが含まれるが、これらに限定されません。HMAC、CMAC、GMAC。有効な暗号強度は少なくとも 128 ビットです（*NIST SP 800-131Ar2*）。 HMAC、CMAC、GMAC の詳細については、それぞれ以下を参照してください。*NIST SP 800-107r1*、*NIST SP 800-38B*、*NIST SP 800-38D*）。 *NIST SP 800-107 (リビジョン 1) を参照してください。承認されたハッシュアルゴリズムを使用するアプリケーションのための推奨事項§5.3 を参照のこと。*
最小特権	職務上の役割と責任を果たすために必要な最小レベルの権限です。
参加ペイメントブランド	"ペイメントブランド "とも呼ばれます。 当該時点において、PCI SSC の運営文書に基づき、その後正式にメンバーとして認められている（またはアフィリエイトとして認められている）ペイメントカードブランドです。本稿執筆時点では、参加支払ブランドには PCI SSC の創立メンバーおよび戦略的メンバーが含まれます。
磁気ストライプデータ	*トラックデータ*を参してください。
商用オフザシェルフ (COTS)	特定の顧客またはユーザ向けに特別にカスタマイズまたは設計されていない在庫品であり、容易に使用できる製品の説明です。
消費者	商品、サービス、またはその両方を購入する個人のカード所有者です。

用語	定義
職務の分離（Separation of Duties）	一人の人間がプロセスを破壊することを防ぐために、ある機能のステップを複数の人間に分割することです。
信頼できるネットワーク	事業体のネットワークで、事業体の管理能力の範囲内にあり、適用される PCI DSS 要件を満たすものです。
人事担当者	アカウントデータを保護するためのセキュリティ責任を負う、またはアカウントデータのセキュリティに影響を与える可能性のある正社員、パートタイム社員、派遣社員、請負業者、コンサルタントです。
脆弱性（ぜいじゃくせい）	悪用された場合、意図的または非意図的にシステムを危険にさらす可能性のある欠陥または弱点です。
組織的独立性	活動を行う人または部署と、活動を評価する人または部署との間に利害の対立がないことを保証する組織構造です。例えば、評価を行う個人は、評価対象の環境の管理者とは組織的に別です。
多要素認証	少なくとも 2 つの要素を検証することにより、ユーザを認証する方法です。これらの要素には、ユーザが持っているもの（スマートカードやドングルなど）、ユーザが知っているもの（パスワード、パスフレーズ、PIN など）、またはユーザ自身やユーザの行動（指紋やその他の生体認証要素など）が含まれます。
ターゲットリスク分析	PCI DSS の目的のために、特定の PCI DSS 要件に焦点を当てたリスク分析。要件が（頻度などの）柔軟性を認めているため、またはカスタマイズアプローチのために、事業体がリスクを評価し、カスタマイズされたコントロールが PCI DSS 要件の目的を満たすと判断した方法を説明するために行われます。
定義されたアプローチ	*PCI DSS の要件とセキュリティ評価手順*の「PCI DSS の実装と検証のためのアプローチ」を参照してください。
特権ユーザ	基本的なアクセス権限よりも大きな権限を持つユーザアカウントのことです。通常、これらのアカウントは、標準的なユーザアカウントよりも多くの権限を持つ昇格または増加した特権を持ちます。ただし、組織、職務、役割、使用する技術によって、特権アカウント間の権限の範囲が大きく異なる場合があります。

用語	定義
認証	個人、装置、またはプロセスの身元を確認するプロセス。認証は通常、1 つまたは複数の認証要素で行われます。*アカウント*、*認証クレデンシャル*、および*認証要素*を参照のことです。
認証／オーソリゼーション	アクセス制御の文脈では、認可は、ユーザ、プログラム、またはプロセスに対するアクセスまたはその他の権利の付与です。認可は認証に成功した後に個人またはプログラムが何ができるかを定義します。 ペイメントカードトランザクションの文脈では、オーソリゼーションは、マーチャントがトランザクション応答（例えば、承認または拒否）を受信したときに完了するオーソリゼーションプロセスを指します。
認証クレデンシャル	ユーザ ID またはアカウント ID と、個人、デバイス、またはプロセスを認証するために使用される認証要素(複数可)の組み合わせです。*アカウント*と*認証要素*を参照してください。
認証要素	コンピュータシステム上で個人またはプロセスの身元を証明または検証するために使用される要素です。認証は通常、以下の認証要素のうち 1 つ以上を用いて行われます。 • パスワードやパスフレーズなど、知っているもの。 • トークンデバイスやスマートカードなど、あなたが持っているもの • バイオメトリクス要素など、あなた自身が持つもの。 ID（またはアカウント）と認証要素を合わせて、認証クレデンシャルと見なされます。 *アカウント*、*認証クレデンシャルを参照してください。*
イシュイングサービス	イシュイングサービスの例としては、オーソリゼーション、カードパーソナライゼーションなどが挙げられるが、これらに限定されません。
イシュア	「発行銀行」または「発行金融機関」とも呼ばれます。発行銀行や発行プロセサーなど、ペイメントカードを発行し、発行サービスを実施、促進、または支援する事業体です。ただし、これらに限定されません。
信頼できないネットワーク	"信頼できるネットワーク "の定義に合致しないネットワークです。
物理的アクセス制御	物理的な空間や環境へのアクセスを、許可された者だけに制限する仕組みです。*論理的アクセス制御*を参照してください。

用語	定義
変更管理	システムおよびソフトウェアの変更について、実施前にその影響を検討し、テストし、承認するためのプロセスおよび手順です。
代替コントロール	*PCI DSS 付録B およびC を参照*
論理的アクセス制御	情報または情報処理資源を、許可された者またはアプリケーションのみが利用できるように制限する仕組みのことです。*物理的アクセス制御*を参照してください。